ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACION, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

CENTRO DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA DE SISTEMAS

TEMA: "ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN APLICADO A LA COMPAÑÍA PROCESADORA NACIONAL DE ALIMENTOS C.A., QUE PERMITA MEJORAR LA ADMINISTRACIÓN DEL DEPARTAMENTO DE TECNOLOGÍA E INFORMACIÓN"

AUTOR: GUAGALANGO VEGA, RICARDO NAPOLEÓN

DIRECTOR: ING. ARROYO CHANGO, RUBÉN DARIO MSc.

SANGOLQUÍ

2017

CERTIFICADO DEL DIRECTOR DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN APLICADO A LA COMPAÑÍA PROCESADORA NACIONAL DE ALIMENTOS C.A., QUE PERMITA MEJORAR LA ADMINISTRACIÓN DEL DEPARTAMENTO DE TECNOLOGÍA E INFORMACIÓN"***, realizado por el señor ***RICARDO GUAGALANGO VEGA***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor ***RICARDO GUAGALANGO VEGA*** para que lo sustente de forma pública.

Ciudad, 11 de agosto del 2017

RUBÉN DARIO ARROYO CHANGO
DIRECTOR DE TESIS

OFICIO DE AUTORÍA DE RESPONSABILIDAD

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORÍA DE RESPONSABILIDAD

Yo, ***RICARDO GUAGALANGO VEGA***, con cédula de identidad N° 1718122474, declaro que este trabajo de titulación ***"ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN APLICADO A LA COMPAÑÍA PROCESADORA NACIONAL DE ALIMENTOS C.A., QUE PERMITA MEJORAR LA ADMINISTRACIÓN DEL DEPARTAMENTO DE TECNOLOGÍA E INFORMACIÓN"***, ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Adicional declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Ciudad, 01 de septiembre del 2017

RICARDO NAPOLÉON GUAGALANGO VEGA
C.C 1718122474

OFICIO DE AUTORIZACIÓN

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, ***RICARDO GUAGALANGO VEGA***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN APLICADO A LA COMPAÑÍA PROCESADORA NACIONAL DE ALIMENTOS C.A., QUE PERMITA MEJORAR LA ADMINISTRACIÓN DEL DEPARTAMENTO DE TECNOLOGÍA E INFORMACIÓN"***, cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Ciudad, 01 de septiembre del 2017

RICARDO NAPOLÉON GUAGALANGO VEGA
C.C 1718122474

DEDICATORIA

El presente trabajo está dedicado a Dios por todas las bendiciones que derrama en mi vida y ser la persona y profesional que soy; además por aprender de sus enseñanzas bíblicas, entre ellas "*Diga el débil, Fuerte Soy*", lo que me ha permitido alcanzar grandes triunfos en todos los campos de mi vida.

Además, agradezco a mis dos pilares que son mis padres: Rosita Vega y Luis Guagalango quienes han forjado en mí, una mejor persona; adicional fueron mi inspiración y fortaleza que necesité en todo momento.

RICARDO NAPOLEÓN GUAGALANGO VEGA

AGRADECIMIENTO

En primer lugar, agradezco a Dios que es quien me ha dado lo más importante que es la vida y me ha sabido dar aliento en los peores momentos.

Agradezco a mis padres ROSITA VEGA Y LUIS GUAGALANGO, ya que ellos fueron quienes me apoyaron en todo momento, y me brindaron todo su amor.

A mis hermanos y familiares que me supieron dar consejos muy valiosos en los momentos más difíciles, lo cual me sirvió para salir adelante.

Al Ingeniero RUBÉN ARROYO, quien con su apoyo supo guiarme para la culminación de este trabajo.

A la universidad donde fui formado y a mis maestros que fueron más que docentes amigos en toda mi carrera profesional.

A todas las personas que son parte de este éxito.

RICARDO NAPOLEÓN GUAGALANGO VEGA

ÍNDICE GENERAL

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, las amenazas y vulnerabilidades han tenido un rápido crecimiento en el mundo tecnológico; teniendo en cuenta que el desarrollo de las estrategias a nivel de seguridad de información comprende tres campos fundamentales: personas, procesos y tecnología, por lo cual las empresas se ven en la necesidad de identificar mediante el concepto de Pareto el nivel prioritario de seguridad, es decir identificar el veinte por ciento (20%) de la información que genera beneficios en la Organización y que facilita la operaciones en un ochenta por ciento (80%). Para llegar a comprender qué información se debe proteger de posibles amenazas y vulnerabilidades se debe realizar un análisis de riesgos que permita gestionar los incidentes de forma proactiva y dar un adecuado tratamiento en el proceso ya que el principal objetivo es degradar los activos de información que generan valor para la Organización, y adicional a los sistemas de información. El presente proyecto se utilizó la Metodología de Análisis y Gestión de Riesgos MAGERIT V3., la cual contempla una herramienta para automatizar el trabajo denominada PILAR. Adicional se contempló la Norma Internacional ISO 27000 y los resultados obtenidos fue la identificación de dos activos de información críticos/sensibles: ERP Infor LN y las Bases de Datos; adicional se determinó que los dominios de la Norma que más carecen de controles son: Política de Seguridad de la Información, Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información y Gestión de los Aspectos de la Seguridad de la Información para la Continuidad del Negocio.

PALABRAS CLAVE:

- **SEGURIDAD DE INFORMACIÓN**
- **ANÁLISIS DE RIESGOS**
- **ACTIVOS DE INFORMACIÓN**

ABSTRACT

Nowadays, threats and vulnerabilities have been rapidly growing in the technological world; considering that the development of strategies at the level of information security comprises three fundamental fields: people, processes and technology, so that companies need identifying through the concept of Pareto the priority level of security, that is, to identify twenty percent (20%) of the information that generates benefits in the Organization and that facilitates the operations in eighty percent (80%). To understand what information should be protected against possible threats and vulnerabilities, a risk analysis must be carried out that allows to manage the incidents proactively and give an adequate treatment in the process since the main objective is to degrade the information that generate value for the Organization, and in addition to information systems. The present project used Risk Analysis and Management Methodology MAGERIT V3, which includes a tool to automate the work called PILAR. Additionally, the International Standard ISO 27000 was considered and the results obtained were the identification of two critical / sensitive information assets: ERP Infor LN and Databases; Additional it was determined that the domains of the Standard that lack the most controls are: Information Security Policy, Acquisition, Development and Maintenance of Information Systems and Management of Aspects of Information Security for Business Continuity.

KEYWORDS:

- **INFORMATION SECURITY**
- **RISK ANALYSIS**
- **INFORMATION ASSETS**

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1 Antecedentes

Las organizaciones ecuatorianas cada vez se alistan para ir al negocio digital; sin embargo, muchas de ellas son empresas reactivas en temas de Seguridad de Información e implementan soluciones informáticas que incurren en gastos significativos y la alta dirección considera un gasto no reflejado en retorno de inversión y la Compañía Multinacional Procesadora Nacional de Alimentos C.A., denominada en adelante Pronaca C.A., no es la excepción. Para poder justificar al Negocio de futuras inversiones en temas relacionados a Seguridad de Información se lo debe realizar midiendo el retorno de inversión en seguridad o ROSI; esto se logra analizando los beneficios económicos que se relacionan a dichas inversiones a través de un análisis de riesgos cuya finalidad es evidenciar las vulnerabilidades y amenazas que posee la empresa y las medidas de seguridad que permitirá prevenir o evitar, considerando el impacto económico reducido gracias a la implantación de medidas y controles que permitirán prevenir o mitigar riesgos informáticos, sin embargo en la última década estos riesgos han aumentado y se han evidenciado en múltiples observaciones de auditoría, como principal responsabilidad del departamento de Tecnología e Información, mismas que han carecido de un debido tratamiento. De igual manera, las distintas evaluaciones realizadas a la plataforma tecnológica han evidenciado múltiples debilidades sin ningún plan de acción para remediar y/o fortalecer el equipamiento TI de la Compañía.

1.2 Planteamiento del problema

Los constantes cambios tecnológicos hacen que la Organización, esté sometida a riesgos, vulnerabilidades y amenazas informáticas tales como: hackers, programas maliciosos e incluso usuarios internos considerados de

mayor peligro, que pueden afectar de manera directa a la información corporativa.

La Compañía Pronaca no ha realizado un análisis de riesgos por más de una década lo que conlleva al desconocimiento de la Dirección de Tecnología e Información de riesgos potenciales que pueden degradar a los activos de información en disponibilidad, integridad y confidencialidad al corto, mediano y largo plazo pudiendo impactar a los estados financieros de la Compañía.

1.3 Justificación

En la actualidad las empresas y organizaciones de cualquier índole deben considerar dentro de sus planes de gobierno el aseguramiento y cumplimiento de estándares que aseguren la información, al ser uno de los principales activos de la Organización.

El presente proyecto se sustenta debido a que, en las revisiones de firmas auditoras y consultorías realizadas a la Compañía en los últimos años, han evidenciado no conformidades que generan riesgos en la seguridad de información.

Considerando que gran parte de la información corporativa se encuentra en equipos de los colaboradores de la Organización, en buzones de correo, en formato físico y en especial almacenada en sistemas de información. En este contexto, es indispensable realizar el análisis de riesgos de seguridad de la información que permita generar conocimiento de las principales amenazas y vulnerabilidades de los activos empresariales que podrían explotarse y materializarse en riesgos; a priori establecer medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad y el fortalecimiento de la integridad, confidencialidad y disponibilidad de la información.

Se utilizará la norma ISO/IEC 27002 la cual es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información y en complemento con la Metodología Magerit para el análisis y gestión de riesgos, que a su vez permite utilizar una herramienta denominada Pilar para automatizar el trabajo a realizarse.

1.4 Objetivo general

Realizar el análisis de riesgos que permita establecer controles y recomendaciones para mitigar los riesgos asociados con vulnerabilidades y amenazas de seguridad de información, existentes en el departamento de Tecnología e Información de la Compañía Pronaca C.A.

1.5 Objetivos específicos

- Realizar una evaluación de la situación actual de Seguridad de Información en el departamento de Tecnología e Información aplicando los controles de la Norma ISO 27001.

- Utilizar la herramienta software PILAR la cual soporta el análisis de riesgos mediante la metodología Magerit V3.

- Sugerir salvaguardas o recomendaciones que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos.

- Elaborar un informe de recomendaciones donde se evidencie los principales hallazgos y grado de criticidad que podrían materializarse al carecer de un tratamiento de mitigación.

1.6 Alcance

El alcance del proyecto consiste en la entrega documentada de un Análisis de Riesgos del departamento de Tecnología e Información el cual identifique amenazas que pueden perjudicar los activos de información, así como recomendaciones que permitan proteger a la Compañía de vulnerabilidades y riesgos que pueden materializarse en el corto, mediano o largo plazo.

CAPÍTULO II

MARCO TEÓRICO Y ESTADO DEL ARTE

El presente trabajo comprende definiciones y conceptos que deben ser entendidos, a continuación se describe los principales términos utilizados y la Norma a aplicarse.

2.1 Norma ISO 27000

Según (Mifsud, 2012), la Seguridad de Información comprende técnicas, organizativas y legales las cuales permiten a una Organización asegurar la confidencialidad, integridad y disponibilidad de los sistemas de información.

El proyecto contempla la utilización de la norma ISO 27000, siendo un conjunto de estándares que suministran un marco de gestión de la seguridad de la información y puede ser utilizada por cualquier tipo de Organización (ISO 27000, 2012).

Dentro de esta extensa norma internacional se describe estándares que soportan a la Seguridad de Información de una Organización, se destaca las siguientes:

Acorde con (Academy 27001, 2016), las normas ISO/IEC 27001 describe cómo gestionar la seguridad de la información en una empresa y la ISO/IEC 27002 se refiere los dominios y controles que puede ser implementados dentro de una Organización con el objetivo principal de mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos expuesto en una Organización (Gutiérrez, 2013).

En la tabla 1, se muestra los Dominios que posee la Norma ISO 27002, divididos de la siguiente manera:

Tabla 1
Dominios ISO 27002

Dominio
a. Políticas de seguridad
b. Aspectos organizativos de la seguridad de la información
c. Seguridad ligada a los recursos humanos.
d. Gestión de activos
e. Control de accesos
f. Cifrado
g. Seguridad física y ambiental
h. Seguridad en la operativa
i. Seguridad en las telecomunicaciones
j. Adquisición, desarrollo y mantenimiento de los sistemas de información
k. Relaciones con suministradores
l. Gestión de incidentes en la seguridad de la información
m. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
n. Cumplimiento

Fuente: (ISO 27001, 2013)

2.2 Dominio de norma ISO 27002

De acuerdo al portal de la Norma ISO en español (ISO 27000, 2012) establece que cada dominio contempla los siguientes objetivos:

a. Política de Seguridad de Información. - Este dominio es una guía de apoyo para la alta Dirección referente a la Seguridad de Información y relaciona los requisitos del negocio, leyes y regulaciones más importantes (ISO 27001, 2013), como se visualiza en la tabla 2, se deben aplicar los siguientes controles a este dominio:

Tabla 2
Dominio Políticas de Seguridad

Dominio: Políticas de seguridad
Objetivo de Control: Directrices de la Dirección en seguridad de la información.
Controles aplicables: • Conjunto de políticas para la seguridad de la información. • Revisión de las políticas para la seguridad de la información.

Fuente: (ISO 27001, 2013)

b. Aspectos organizativos de la seguridad de la información. - Se enfoca en el establecimiento de una estructura de gestión con la finalidad de implementar de mejor manera la Seguridad de Información, empezando por la aprobación de la política y asignado roles de seguridad y segregando tareas en toda la Compañía. Es importante tener contactos con especialistas de seguridad y de esa manera están actualizado de nuevas tendencias en este campo (ISO 27001, 2013).

Como punto adicional y ayuda a la gestión se puede crear un Comité de Seguridad para que exista el apoyo de la Alta Dirección. Como se observa en la tabla 3, se deben aplicar controles referentes a la organización interna y dispositivos para movilidad y teletrabajo:

Tabla 3
Dominio Aspectos de la seguridad de la información

Dominio: Aspectos organizativos de la seguridad de la información
Objetivo de Control: Organización interna.
Controles aplicables: • Asignación de responsabilidades para la segur. de la información • Segregación de tareas • Contacto con las autoridades • Contacto con grupos de interés especial

CONTINÚA

• Seguridad de la información en la gestión de proyectos
Objetivo de Control: Dispositivos para movilidad y teletrabajo
Controles aplicables: • Política de uso de dispositivos para movilidad • Teletrabajo

Fuente: (ISO 27001, 2013)

c. Seguridad ligada a los recursos humanos. - Persigue el aseguramiento a empleados, contratistas y terceros para que entiendan sus responsabilidades dentro de la Organización, esto con el objetivo de reducir posibles incidentes como: robos, fraudes o mal uso de los activos de información (ISO 27001, 2013).

Para realizar esta gestión es relevante trabajar con el área de Talento Humano y establecer responsabilidades, antes, durante y después de una contratación de un colaborador con la debida formalización y acuerdos de confidencialidad.

La tabla 4, muestra los controles que se deben aplicar a este dominio:

Tabla 4
Dominio Seguridad ligada a los recursos humanos

Dominio: Seguridad ligada a los recursos humanos
Objetivo de Control: Antes de la contratación
Controles aplicables: • A Investigación de antecedentes • Términos y condiciones de contratación
Objetivo de Control: Durante la contratación
Controles aplicables: • Responsabilidades de gestión • Concienciación, educación y capacitación en seguridad de la información • Proceso disciplinario
Objetivo de Control: Cese o cambio de puesto de trabajo
Controles aplicables: • Cese o cambio de puesto de trabajo.

Fuente: (ISO 27001, 2013)

d. Gestión de Activos. - Tiene como finalidad justificar la asignación de un activo de la Compañía a un propietario, adicional se debe establecer responsabilidades de la adecuada protección del bien.

Para tener un mejor control es necesario tener un inventario de activos de información actualizado, inclusive se puede usar códigos de barras para facilitar las tareas de ingreso y salida de activos de las instalaciones de la Compañía (ISO 27001, 2013). Como se visualiza en la tabla 5, existen tres objetivos de controles que deben considerarse:

Tabla 5
Dominio Gestión de activos

Dominio: Gestión de activos
Objetivo de Control: Responsabilidad sobre los activos
Controles aplicables: • Inventario de activos. • Propiedad de los activos. • Uso aceptable de los activos. • Devolución de activos.
Objetivo de Control: Clasificación de la información
Controles aplicables: • Directrices de clasificación • Etiquetado y manipulado de la información • Manipulación de activos
Objetivo de Control: Manejo de los soportes de almacenamiento
Controles aplicables: • Gestión de soportes extraíbles. • Eliminación de soportes. • Soportes físicos en tránsito.

Fuente: (ISO 27001, 2013)

e. Control de Accesos. - Se debe realizar con base a las políticas de distribución de información y con la debida autorización. De la misma manera los propietarios de los activos son los custodios y responsables del acceso a su información (ISO 27001, 2013).

Como se observa en la tabla 6, existen varios controles que la Compañía debe aplicar con la finalidad de proteger el control de accesos:

Tabla 6
Dominio Control de accesos

Dominio: Control de accesos
Objetivo de Control: Requisitos de negocio para el control de accesos
Controles aplicables: • Política de control de accesos. • Control de acceso a las redes y servicios asociados.
Objetivo de Control: Gestión de acceso de usuario
Controles aplicables: • Gestión de altas/bajas en el registro de usuarios • Gestión de los derechos de acceso asignados a usuarios • Gestión de los derechos de acceso con privilegios especiales • Gestión de información confidencial de autenticación de usuarios • Revisión de los derechos de acceso de los usuarios • Retirada o adaptación de los derechos de acceso
Objetivo de Control: Responsabilidades del usuario
Controles aplicables: • Uso de información confidencial para la autenticación
Objetivo de Control: Control de acceso a sistemas y aplicaciones
• Restricción del acceso a la información • Procedimientos seguros de inicio de sesión • Gestión de contraseñas de usuario • Uso de herramientas de administración de sistemas • Control de acceso al código fuente de los programas

Fuente: (ISO 27001, 2013)

f. Cifrado. - Se refiere al establecimiento de una política de uso de controles criptográficos y gestión de claves.

Como se ve en la tabla 7, se deben aplicar dos controles para fortalecer el cifrado en la Compañía:

Tabla 7
Dominio Cifrado

Dominio: Cifrado
Objetivo de Control: Controles criptográficos
Controles aplicables: • Política de uso de los controles criptográficos • Gestión de claves

Fuente: (ISO 27001, 2013)

g. Seguridad física y ambiental. - Busca evitar accesos físicos no autorizados o posibles daños a las instalaciones y a la información de la Compañía. También enfatiza que los servicios de procesamiento de la información de carácter confidencial y sensible, deben ubicarse en área protegidas estableciendo controles de entrada (ISO 27001, 2013).

Como se visualiza en la tabla 8 se debe aplicar los siguientes controles para fortalecer la seguridad perimetral:

Tabla 8
Dominio Seguridad física y ambiental

Dominio: Seguridad física y ambiental
Objetivo de Control: Áreas seguras
Controles aplicables: • Perímetro de seguridad física • Controles físicos de entrada • Seguridad de oficinas, despachos y recursos • Protección contra las amenazas externas y ambientales • El trabajo en áreas seguras • Áreas de acceso público, carga y descarga
Objetivo de Control: Seguridad de los equipos.
Controles aplicables:

CONTINÚA

• Emplazamiento y protección de equipos • Instalaciones de suministro • Seguridad del cableado • Mantenimiento de los equipos • Salida de activos fuera de las dependencias de la empresa • Seguridad de los equipos y activos fuera de las instalaciones • Reutilización o retirada segura de dispositivos de almacenamiento • Equipo informático de usuario desatendido • Política de puesto de trabajo despejado y bloqueo de pantalla

Fuente: (ISO 27001, 2013)

h. Seguridad en la operativa. - Este dominio se centra en la gestión de cambios, capacidades, y la debida separación de ambientes de desarrollo, prueba y producción. Adicional establece que en la Organización debe existir copias de seguridad (ISO 27001, 2013).

A continuación, la tabla 9, presenta los controles aplicables a este dominio:

Tabla 9
Dominio Seguridad en la operativa

Dominio: Seguridad en la operativa
Objetivo de Control: Responsabilidades y procedimientos de operación
Controles aplicables: • Documentación de procedimientos de operación • Gestión de cambios • Gestión de capacidades • Separación de entornos de desarrollo, prueba y producción
Objetivo de Control: Protección contra código
Controles aplicables: • Controles contra el código malicioso
Objetivo de Control: Copias de seguridad
Controles aplicables:

CONTINÚA

• Copias de seguridad de la información
Objetivo de Control: Registro de actividad y supervisión
Controles aplicables: • Registro y gestión de eventos de actividad • Protección de los registros de información • Registros de actividad del administrador y operador del sistema • Sincronización de relojes
Objetivo de Control: Control del software en explotación
Controles aplicables: • Instalación del software en sistemas en producción
Objetivo de Control: Gestión de la vulnerabilidad técnica
Controles aplicables: • Gestión de las vulnerabilidades técnicas • Restricciones en la instalación de software
Objetivo de Control: Consideraciones de las auditorías de los sistemas de información
Controles aplicables: • Controles de auditoría de los sistemas de información

Fuente: (ISO 27001, 2013)

i. Seguridad en las telecomunicaciones. - Este dominio que se enfoca a la gestión de la seguridad de las redes, en ello se instaura la debida segregación y mecanismo de seguridad asociados a servicios en red. También considera que se debe tener políticas y procedimientos para el intercambio de información con partes externas (ISO 27001, 2013).

Como se observa en la tabla 10, se deben considerar controles relacionados a la gestión de la seguridad en las distintas redes de la Compañía y el intercambio de información con partes externas:

Tabla 10
Dominio Seguridad en las telecomunicaciones

Dominio: Seguridad en las telecomunicaciones
Objetivo de Control: Gestión de la seguridad en las redes
Controles aplicables: • Controles de red • Mecanismos de seguridad asociados a servicios en red • Segregación de redes
Objetivo de Control: Intercambio de información con partes externas
Controles aplicables: • Políticas y procedimientos de intercambio de información • Acuerdos de intercambio • Mensajería electrónica • Acuerdos de confidencialidad y secreto

Fuente: (ISO 27001, 2013)

j. Adquisición, desarrollo y mantenimiento de los sistemas de información. - *C*onsidera que, dentro del campo de los sistemas de información, donde se involucra a sistemas operativos, aplicaciones, infraestructura, servicios, entre otros, son importantes para la consecución de los objetivos corporativos. Por lo cual es importante considerar requisitos de seguridad a ser identificados y consensuados con antelación al desarrollo o a la implementación de los sistemas de información (ISO 27001, 2013).

La tabla 11, muestra los controles que se deben aplicarse en este dominio:

Tabla 11
Dominio Mantenimiento de los sistemas de información

Dominio: Adquisición, desarrollo y mantenimiento de los sistemas de información
Objetivo de Control: Requisitos de seguridad de los sistemas de información
Controles aplicables: • Análisis y especificación de los requisitos de seguridad • Seguridad de las comunicaciones en servicios accesibles por redes públicas • Protección de las transacciones por redes telemáticas
Objetivo de Control: Seguridad en los procesos de desarrollo y soporte
Controles aplicables: • Política de desarrollo seguro de software • Procedimientos de control de cambios en los sistemas • Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo • Restricciones a los cambios en los paquetes de software • Uso de principios de ingeniería en protección de sistemas • Seguridad en entornos de desarrollo • Externalización del desarrollo de software • Pruebas de funcionalidad durante el desarrollo de los sistemas • Pruebas de aceptación
Objetivo de Control: Datos de prueba
• Protección de los datos utilizados en pruebas

Fuente: (ISO 27001, 2013)

k. Relaciones con suministradores. - *S*e enfoca en la supervisión, revisión y gestión de cambios en los servicios prestados por terceros (ISO 27001, 2013).

La Compañía debe verificar la implementación de acuerdos y el debido cumplimiento.

Como se muestra en la tabla 12, los controles aplicables al dominio son los siguientes:

Tabla 12
Dominio Relaciones con suministradores

Dominio: Relaciones con suministradores
Objetivo de Control: Seguridad de la información en las relaciones con suministradores
Controles aplicables: • Política de seguridad de la información para suministradores • Tratamiento del riesgo dentro de acuerdos de suministradores • Cadena de suministro en tecnologías de la información y comunicaciones
Objetivo de Control: Gestión de la prestación del servicio por suministradores
Controles aplicables: • Supervisión y revisión de los servicios prestados por terceros • Gestión de cambios en los servicios prestados por terceros

Fuente: (ISO 27001, 2013)

I. Gestión de incidentes en la seguridad de la información. - Garantiza que posibles eventos negativos o debilidades en la seguridad relacionadas con los sistemas de información, tengan una pronta comunicación de forma tal que se pueda efectuar acciones correctivas.

Es importante que dentro de esta gestión se establezca informe de los eventos suscitados y el procedimiento de escalamiento realizado, tomando en consideración que todos los empleados, contratistas y/o terceros conozcan sobre las acciones realizadas (ISO 27001, 2013).

Como se visualiza en la tabla 13, los controles que se deben considerar para mejorar la gestión de incidentes de seguridad de la información en la Organización son los siguientes:

Tabla 13
Dominio Gestión de incidentes

Dominio: Gestión de incidentes en la seguridad de la información
Objetivo de Control: Gestión de incidentes de seguridad de la información y mejoras
Controles aplicables: • Responsabilidades y procedimientos • Notificación de los eventos de seguridad de la información • Notificación de puntos débiles de la seguridad • Valoración de eventos de seguridad de la información y toma de decisiones • Respuesta a los incidentes de seguridad • Aprendizaje de los incidentes de seguridad de la información • Recopilación de evidencias

Fuente: (ISO 27001, 2013)

m. Aspectos de seguridad de la información en la gestión de la continuidad del negocio. - Centra sus esfuerzos en la implementación de un proceso de gestión para la continuidad del negocio con el fin de reducir a un nivel aceptable, la interrupción a causa de posibles desastres naturales y fallos de seguridad, contemplando medidas preventivas y de recuperación (ISO 27001, 2013).

Como se muestra en la tabla 14, los controles que deben aplicarse para mejorar la continuidad de Negocio en la Compañía son los siguientes:

Tabla 14
Dominio Aspectos de Gestión de la continuidad del negocio

Dominio: Aspectos de seguridad de la información en la gestión de la continuidad del negocio
Objetivo de Control: Continuidad de la seguridad de la información
Controles aplicables: • Planificación de la continuidad de la seguridad de la información • Implantación de la continuidad de la seguridad de la información • Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Objetivo de Control: Redundancias
• Disponibilidad de instalaciones para el procesamiento de la información

Fuente: (ISO 27001, 2013)

n. Cumplimiento. - Su principal objetivo es evitar incumplir leyes, estatutos, regulaciones u obligaciones contractuales en materia de seguridad. Es necesario que la Organización se apoye de asesores legales o profesionales calificados que ayuden en temas de requisitos legales (ISO 27001, 2013).

Como se muestra en la tabla 15, se debe contemplar los siguientes controles:

Tabla 15
Dominio Cumplimiento

Dominio: Cumplimiento
Objetivo de Control: Cumplimiento de los requisitos legales y

CONTINÚA

contractuales
Controles aplicables: • Identificación de la legislación aplicable • Derechos de propiedad intelectual (DPI) • Protección de los registros de la organización • Protección de datos y privacidad de la información personal • Regulación de los controles criptográficos
Objetivo de Control: Revisiones de la seguridad de la información
• Revisión independiente de la seguridad de la información • Cumplimiento de las políticas y normas de seguridad • Comprobación del cumplimiento

Fuente: (ISO 27001, 2013)

Es importante mencionar que los controles que cita la norma (ISO 27000, 2012), se pueden aplicar o no dependiendo del tipo de Organización. En otros casos se puede aplicar un tratamiento adecuado de riesgos frente a los controles de la Norma.

2.3 Metodología Magerit

La metodología utilizada para este proyecto es Magerit V3., según (Portal Administración Electrónica, 2012) permite realizar análisis y gestión de riesgos; en primera instancia implementa el proceso de gestión de riesgos el mismo que facilita la toma decisiones considerando los riesgos que involucran del uso de tecnologías de la información.

Acorde con (Amutio, 2012), la metodología apremia los siguientes objetivos:

Directos:

- Existencia de riesgos en una Organización y la debida concientización a los encargados y/o responsables de que se debe gestionar de manera adecuada.

- Realizar análisis de riegos estableciendo un método sistemático.
- Planificar de forma oportuna y con ello mantener los riesgos potenciales a un nivel aceptable.

Indirectos:

- Alistar a la Organización ante revisiones de firmas auditoras o consultorías de cara a una certificación o acreditación.

Como se muestra en la Figura 1. y según (Amutio, 2012), las fases para realizar el análisis se distribuyen de la siguiente forma:

1. Identificar los activos con mayor relevancia y valor para la Organización, y qué perjuicio o coste causaría al degradasen.
2. Establecer amenazas a los que se exponen los activos identificados.
3. Determinar las salvaguardas o recomendaciones mitigarían las amenazas y la eficacia ante los riesgos.
4. Estimar el impacto, el cual se define como daños sobre el activo a causa de la materialización de una amenaza
5. Valorar el riesgo, usando la fórmula de impacto ponderado con la tasa de ocurrencia de la amenaza.

También, (Amutio, 2012) establece que un análisis de riesgo contempla los siguientes elementos:

1. Activos, elementos del sistema de información y apoyan la consecución de la misión de la Organización.
2. Amenazas, cosas negativas que les pueden degradar a los activos.
3. Salvaguardas, medidas de protección para que las amenazas identificadas no causen un daño significativo.

Habiendo obtenido aquello elementos se puede estimar:

4. El impacto: “Lo que podría pasar”.
5. El riesgo: “Lo que muy probable pase”.
6. El riesgo residual: Riesgo que subsiste posterior de haber implementado controles.

La figura 1, señala el proceso que realiza la metodología desde la valoración de activos hasta la obtención de riesgos residuales mediante salvaguardas:

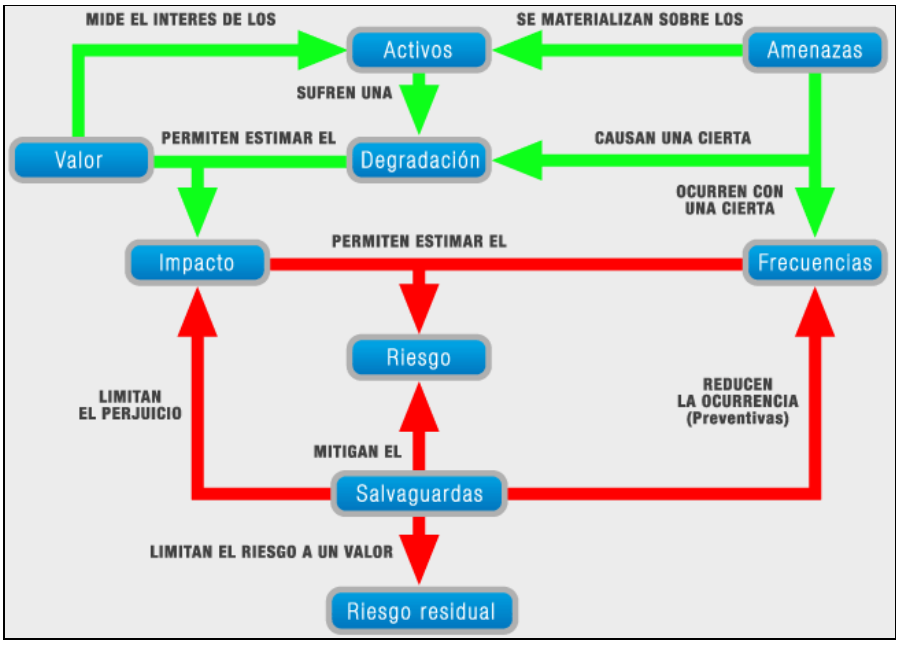


Figura 1 Metodología de Análisis de Riesgos

Fuente: *(Ramos, 2012)*

Los términos básicos del estudio de las variables planteadas y definiciones que serán utilizadas en el presente proyecto se resumen a continuación:

Según (González, 2012), el análisis de riesgos es un proceso para comprender los riesgos y determinar sus niveles, adicional cita que se debe considerar como parte inicial la identificación de activos importantes, los cuales se exponen a amenazas y que al materializarse degradarían a los

mismos, produciendo un impacto. Al estimar la frecuencia con que se materializan amenazas, se puede deducir el riesgo al que está expuesto el sistema.

Según (Isaca, 2011), los activos de Información son un recurso o bien económico que forman parte de una empresa, con el cual se obtienen beneficios y varían de acuerdo con la actividad desarrollada.

La Amenaza es todo suceso negativo con la finalidad de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (Symantc, 2016)

Cabe indicar que (Cappuccio, 2009), menciona que el Impacto mide la consecuencia al materializarse una amenaza; generando Riesgos que son aquellas posibilidades de que una amenaza explote una vulnerabilidad para causar daño en un activo de información (González, 2012).

Acorde con (Aguilera, 2010), las Vulnerabilidades son probabilidades que amenazas se materialicen contra un activo.

Por tal motivo se debe realizar un Estimación de Riesgos para comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable, posterior realizar una Gestión de Riesgos, las cuales contemplen actividades coordinadas para dirigir y controlar los riesgos hasta obtener el Riesgo residual el cual permanece después del tratamiento del riesgo. Esto se puede lograr estableciendo Salvaguardas aplicadas para mitigar riesgos (González, 2012)

Todo este proceso conlleva a la Seguridad de la información con la finalidad de la preservación de los pilares de Seguridad siendo: la confidencialidad, integridad y disponibilidad de la información.

(Mifsud, 2012), asevera que la Confidencialidad es el acceso a la información solo mediante autorización y de forma controlada. La Integridad es la modificación de la información solo mediante autorización y la Disponibilidad hace referencia a que la información del sistema debe permanecer accesible mediante autorización.

Acorde con (González, 2012), considera que se debe proteger la Autenticidad para asegurar que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información se puede tener manipulación del origen o el contenido de los datos o también suplantación de identidad. También, se debe considerar la Trazabilidad para tener un aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento realizó acciones en los activos de información.

Según (Morán, 2012), durante el análisis y gestión de riesgos es importante definir los niveles de riesgos aceptables (NRA) lo cual es un tipo de criterio de aceptación de riesgos (CAR). Es importante que durante la etapa del tratamiento de riesgos la Compañía emplee criterios razonables con los cuales acepte riesgos de niveles no aceptables, la figura 2 muestra los niveles de riesgos y las cuatro (4) maneras de tratar un riesgo:

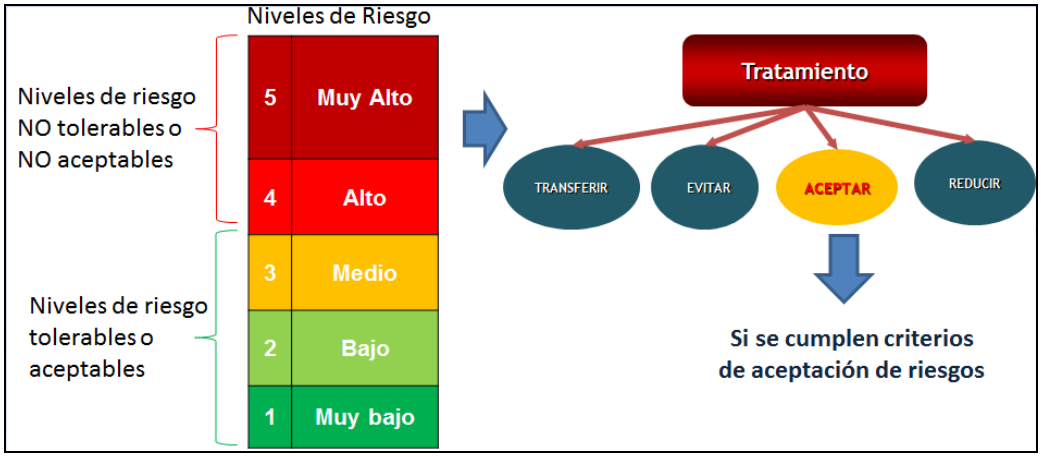


Figura 2 Niveles y tratamiento de riesgos

Fuente: (Morán, 2012)

2.4 Herramienta Pilar

Acorde con el creador de la herramienta PILAR (Mañas, 2012), es un software que complementa a la metodología MAGERIT la cual fue desarrollada por el Centro Criptológico Nacional (CCN), adicional dispone de una biblioteca estándar y es capaz de generar calificaciones respecto a la norma internacional ISO/IEC 27002 Código de buenas prácticas para la Gestión de la Seguridad de la Información

Las variables contempladas serán interpretadas con la ayuda de la herramienta, la cual evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, adicional las salvaguardas se califican por fases.

Para el proyecto se utilizará la última versión de PILAR V.6.2.6, adicional el creador de la Herramienta Dr. Jose A. Mañas, quien ha provisto de una licencia educacional sin costo por un período de seis meses para poder realizar el análisis de riesgos, en este trabajo.

La figura 3, muestra la interfaz de la herramienta PILAR, así como las fases que se contemplarán para el análisis de riesgos:

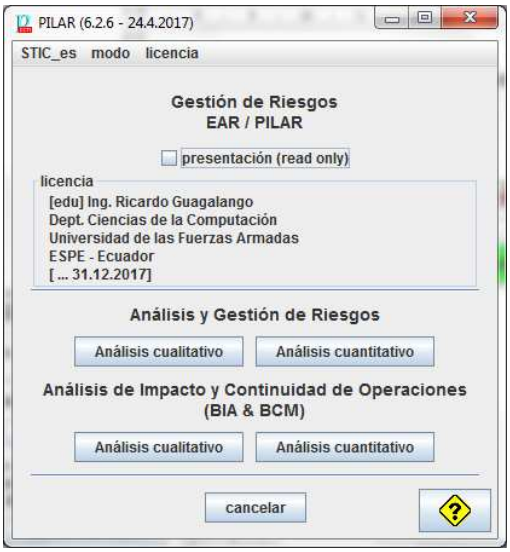
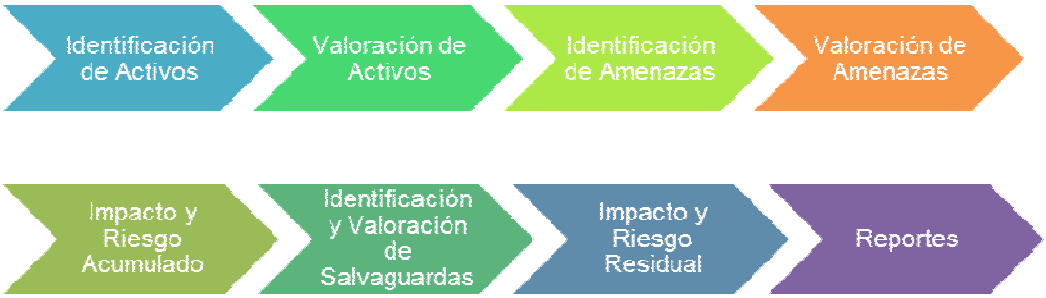


Figura 3 Interfaz de Pilar

A continuación, se muestra el proceso para uso de la herramienta:



Los resultados se presentan en varios formatos y gráficas como: puntos, barras, radar, diagramas de pareto, entre otros. Como ejemplo, se presenta el resultado de cálculo de riesgo en un sistema de información, a lo largo de varias fases del proyecto:

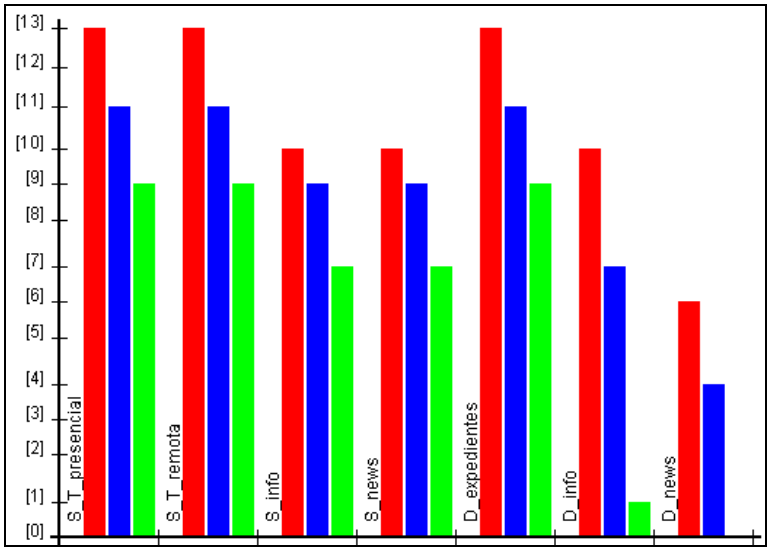


Figura 4 Ejemplo estadístico de Análisis de Riesgos

Fuente: *(Ramos, 2012)*

La figura 5, muestra la evolución del riesgo sobre los activos de tipo servicio y datos:

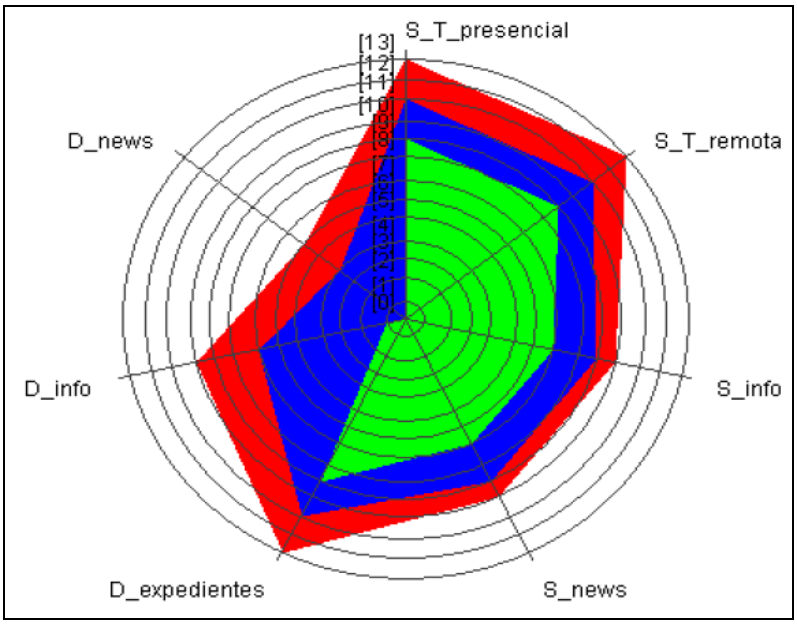


Figura 5 Ejemplo evolutivo de riesgos sobre activos

Fuente: *(Ramos, 2012)*

2.5 Estado del arte

En la actualidad, las empresas son consideradas como sociedades de la información, donde las tecnologías de la información son fundamentales para la continuidad operativa y un factor clave en este campo es la Seguridad de Información debido a que permite proteger uno de los principales activos en cualquier organización: “la información”, ya que de manera continua surgen nuevas amenazas y vulnerabilidades; por ende se han contemplado diferentes análisis de riesgos a nivel local, regional y mundial con el objetivo de mitigar incidencias.

A nivel local, se pueden citar proyectos que realizaron análisis de riesgos utilizando la Metodología Magerit; como es el caso de (Moncayo, 2014) quién realizó un Diseño de un Sistema de Gestión en Control y Seguridad basado en la norma Basc para la Empresa de Transportes y Servicios Asociados Sytsa Cía. Ltda., esto permitió comparar información para la

obtención de impactos y riesgos y el debido tratamiento de acuerdo al grado de criticidad, adicional el establecimiento de políticas y controles para mitigar los riesgos identificados. La metodología ha sido utilizada en otros proyectos semejantes, como el caso de (Rosero, 2014) quién realizó un Análisis de Riesgos de la Seguridad de la Red de Área Local (Lan) de la Matriz de la Contraloría General del Estado y esto permitió identificar los activos con un mayor nivel de riesgo en la organización, debido a la falta de implementación de salvaguardas de seguridad como recomiendan los estándares y código de buenas prácticas para la Gestión de la Seguridad de la Información.

A nivel regional existen proyectos de análisis y gestión de riesgos; (Aguirre, 2013), realizaron un Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la Ofrenda, este estudio permitió determinar los riesgos de la Empresa, adicional clasificar el nivel de impacto de los riesgos y la construcción de planes de mitigación de riesgos. También se han presentado artículos técnicos relacionados (Sotelo, 2012), presentaron un proceso de análisis de riesgos de activos de información, en el contexto de un Sistema de Gestión de Seguridad de Información (SGSI) alineado al estándar ISO/IEC 27001:2005; el mismo que se apoya del marco referencial Magerit (Metodología de Análisis y Gestión de Riesgos de Tecnologías de Información) como eje de la propuesta.

A nivel mundial, en Madrid-España como trabajo de fin de Máster (Molina, 2015), realizó una Propuesta de un Plan de Gestión de Riesgos de Tecnología Aplicado en la Escuela Superior Politécnica del Litoral, concluyendo que la metodología Magerit fue de utilidad para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte del departamento de informática y mediante el análisis de riesgos de orden cualitativo permitió conocer el nivel de madurez en la seguridad aplicada en la institución para sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto.

CAPÍTULO III

DESARROLLO DEL PROYECTO

3.1 Datos de la Compañía

La Empresa que será objeto de estudio para realizar el Análisis de Riesgos es la Compañía Procesadora Nacional de Alimentos C.A. – PRONACA, la cual es una empresa ecuatoriana que se dedica a la producción y distribución de productos alimenticios, siendo una de las empresas más importantes de Agroindustria en Sudamérica.

La Compañía se basa en un propósito: "*Alimentar bien generando desarrollo en el sector agropecuario".*

La cultura de la Compañía se fundamenta en tres valores centrales y son los siguientes:

- Integridad
- Responsabilidad
- Solidaridad

El cumplimiento y aplicación de la Filosofía se basa en los siguientes principios de acción:

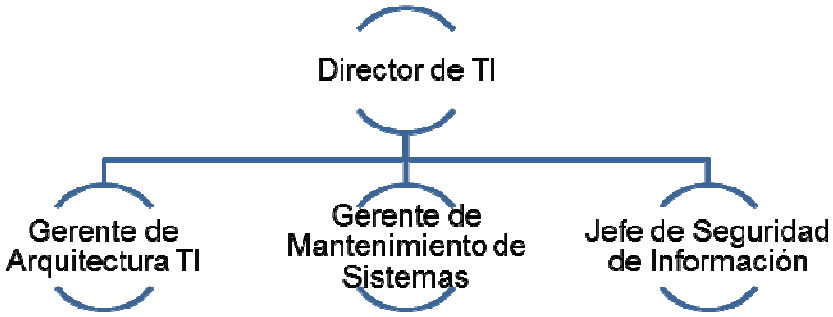
Ser Humanos:

- Desarrollo de Personas
- Coherencia
- Trabajo en Equipo

Ser Eficientes:

- Cambio e innovación
- Respondimiento

Dentro de la Compañía existe un departamento el cual apoya al cumplimiento de los objetivos estratégicos por medio las Tecnología de Información y Comunicaciones, esta área se denomina Tecnología e Información TI y está distribuída en base al siguiente Organigrama:



El presente proyecto contempla realizar el análisis de riesgos al departamento TI, para conocer las principales amenazas y vulnerabilidades que posee. En primera instancia es necesario establecer las metodologías de investigación y técnicas que permitirán estar al tanto de la situación actual del departamento relacionado a Seguridad de Información.

3.2 Metodología de la Investigación

Para cocer la situación actual del departamento es necesario investigar con los distintos Administradores de aplicaciones y bases de datos, Gerentes, Director, entre otros colaboradores, utilizando entrevistas, paneles, encuestas y cuestionarios; para ello se aplicarán las siguientes metodologías de investigación:

Determinístico y cualitativo, considerando aspectos de orden descriptivo. El paradigma de investigación cualitativo permitirá analizar comentarios, ponencias y apreciaciones de los colaboradores de la Compañía.

La información recolectada permitirá establecer un diagnóstico y vulnerabilidades del campo de la seguridad de información de la Compañía.

3.2.1 Técnicas de Investigación

La técnica de investigación para el presente proyecto será: descriptiva correlacional, ya que permitirá identificar las distintas realidades de hecho, datos y resultados obtenidos en la aplicación de las diferentes técnicas e instrumentos de observación aplicados que permitirán obtener una interpretación apropiada de los datos obtenidos.

Este método permitirá integrarse con la investigación exploratoria, misma que facilitará tener una visión global de la problemática de la seguridad de información de la organización.

El trabajo desarrollado se plantea como una investigación descriptiva correlacional cuyo objetivo se centra en la identificación de diferentes situaciones que podrían afectar a la seguridad de información de la Compañía.

3.3 Instrumentos de investigación

Los instrumentos a utilizarse para la obtención de información son:

- Entrevistas con el personal clave de TI
- Encuestas al departamento TI
- Solicitud de documentación vigente y aprobada
- Petición de requerimientos para el análisis de riesgos

Como punto inicial, se mantendrán entrevistas con el personal de Tecnología e Información, con el fin de realizar el relevamiento de información el cual permita obtener un entendimiento general enfocado a la identificación de controles existentes.

Como siguiente punto, se aplicará procedimientos de auditoría basados en indagación, observación e inspección, para probar el diseño, operatividad y razonabilidad de los controles definidos.

Para culminar, la información será validada con los Gerentes del Área TI, con lo cual se evidenciará la vigencia y aprobación, para así garantizar la confiabilidad e integridad de la información entregada. Adicional, estos datos serán ingresados en la herramienta PILAR para proceder a realizar el análisis de riesgos, siguiendo la metodología sistemática Magerit.

3.4 Población y muestra

3.4.1 Población

La población contemplada serán todos los colaboradores del departamento de Tecnología e Información y los activos de información relevantes para la Compañía.

3.4.2 Muestra

Para el caso de estudio no se contemplará muestras; se aplicará encuestas a todo el personal de Tecnología, con el fin de tener un análisis de riesgos global.

3.5 Situación Actual del departamento TI

Para conocer la situación actual del departamento de TI en materia de Seguridad de Información se realizó encuestas, entrevistas, paneles con el personal de Tecnología e Información y el área de Seguridad de Información durante los meses de enero - abril 2017.

Del anexo A de la norma (ISO 27001, 2013), se tomaron los controles y se transformaron a preguntas por cada dominio de la norma y se evidenció si existe un cumplimiento con respuestas de verdadero o falso.

A continuación, se detalla las preguntas realizadas al Departamento de TI y que los Gerentes consideraron aplicables a la realidad de la Compañía:

POLÍTICAS DE SEGURIDAD:

- ¿Existen documento(s) de políticas de seguridad de SI?
- ¿Existe normativa relativa a la seguridad de los SI?
- ¿Existen procedimientos relativos a la seguridad de SI?
- ¿Existe un responsable de las políticas, normas y procedimientos?
- ¿Existen mecanismos para la comunicación a los usuarios de las normas?
- ¿Existen controles regulares para verificar la efectividad de las políticas?

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:

- ¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?
- ¿Existe un responsable encargado de evaluar la adquisición y cambios de SI?

- ¿La Dirección y las áreas de la Organización participa en temas de seguridad?
- ¿Existen condiciones contractuales de seguridad con terceros y outsourcing?
- ¿Existen criterios de seguridad en el manejo de terceras partes?
- ¿Existen programas de formación en seguridad para los empleados,
- clientes y terceros?
- ¿Existe un acuerdo de confidencialidad de la información que se accede?
- ¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?

GESTIÓN DE ACTIVOS:

- ¿Existen un inventario de activos actualizado?
- ¿El Inventario contiene activos de datos, software, equipos y servicios?
- ¿Se dispone de una clasificación de la información según la criticidad de la misma?
- ¿Existe un responsable de los activos?
- ¿Existen procedimientos para clasificar la información?
- ¿Existen procedimientos de etiquetado de la información?

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS:

- ¿Se tienen definidas responsabilidades y roles de seguridad?
- ¿Se tiene en cuenta la seguridad en la selección y baja del personal?
- ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?
- ¿Se imparte la formación adecuada de seguridad y tratamiento de activos?

- ¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?
- ¿Se recogen los datos de los incidentes de forma detallada?
- ¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?
- ¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?
- ¿Existe un proceso disciplinario de la seguridad de la información?

SEGURIDAD FÍSICA Y AMBIENTAL:

- ¿Existe perímetro de seguridad física (una pared, puerta con llave)?
- ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?
- ¿Un área segura ha de estar cerrada, aislada y protegida de eventos naturales?
- ¿En las áreas seguras existen controles adicionales al personal propio y ajeno?
- ¿Las áreas de carga y expedición están aisladas de las áreas de SI?
- ¿La ubicación de los equipos están de tal manera para minimizar accesos innecesarios?
- ¿Existen protecciones frente a fallos en la alimentación eléctrica?
- ¿Existe seguridad en el cableado frente a daños e intercepciones?
- ¿Se asegura la disponibilidad e integridad de todos los equipos?
- ¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?
- ¿Se incluye la seguridad en equipos móviles?

SEGURIDAD EN LAS TELECOMUNICACIONES:

- ¿Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados?

- ¿Están establecidas responsabilidades para controlar los cambios en equipos?
- ¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?
- ¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?
- ¿Existe una separación de los entornos de desarrollo y producción?
- ¿Existen contratistas externos para la gestión de los Sistemas de Información?
- ¿Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?
- ¿Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones?
- ¿Controles contra software maligno?
- ¿Realizar copias de backup de la información esencial para el negocio?
- ¿Existen logs para las actividades realizadas por los operadores y administradores?
- ¿Existen logs de los fallos detectados?
- ¿Existen rastro de auditoría?
- ¿Existe algún control en las redes?
- ¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?
- ¿Eliminación de los medios informáticos?
- ¿Existe seguridad de la documentación de los Sistemas?
- ¿Existen acuerdos para intercambio de información y software?
- ¿Existen medidas de seguridad de los medios en el tránsito?
- ¿Existen medidas de seguridad en el comercio electrónico?
- ¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?
- ¿Existen medidas de seguridad en las transacciones en línea?

- ¿Se monitorean las actividades relacionadas a la seguridad?

CONTROL DE ACCESOS:

- ¿Existe una política de control de accesos?
- ¿Existe un procedimiento formal de registro y baja de accesos?
- ¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?
- ¿Existe una gestión de los password de usuarios?
- ¿Existe una revisión de los derechos de acceso de los usuarios?
- ¿Existe el uso del password?
- ¿Se protege el acceso de los equipos desatendidos?
- ¿Existen políticas de limpieza en el puesto de trabajo?
- ¿Existe una política de uso de los servicios de red?
- ¿Se asegura la ruta (path) desde el terminal al servicio?
- ¿Existe una autenticación de usuarios en conexiones externas?
- ¿Existe una autenticación de los nodos?
- ¿Existe un control de la conexión de redes?
- ¿Existe un control del routing de las redes?
- ¿Existe una identificación única de usuario y una automática de terminales?
- ¿Existen procedimientos de log-on al terminal?
- ¿Se ha incorporado medidas de seguridad a la computación móvil?
- ¿Está controlado el teletrabajo por la organización?

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:

- ¿Se asegura que la seguridad está implantada en los Sistemas de Información?
- ¿Existe seguridad en las aplicaciones?
- ¿Existen controles criptográficos?

- ¿Existe seguridad en los ficheros de los sistemas?
- ¿Existe seguridad en los procesos de desarrollo, testing y soporte?
- ¿Existen controles de seguridad para los resultados de los sistemas?
- ¿Existe la gestión de los cambios en los SO?
- ¿Se controlan las vulnerabilidades de los equipos?

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:

- ¿Se comunican los eventos de seguridad?
- ¿Se comunican las debilidades de seguridad?
- ¿Existe definidas las responsabilidades antes un incidente?
- ¿Existe un procedimiento formal de respuesta?
- ¿Existe la gestión de incidentes?

AASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:

- ¿Existen procesos para la gestión de la continuidad?
- ¿Existe un plan de continuidad del negocio y análisis de impacto?
- ¿Existe un diseño, redacción e implantación de planes de continuidad?
- ¿Existe un marco de planificación para la continuidad del negocio?
- ¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?

CUMPLIMIENTO:

- ¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?
- ¿Existe el resguardo de la propiedad intelectual?
- ¿Existe el resguardo de los registros de la organización?

- ¿Existe una revisión de la política de seguridad y de la conformidad técnica?
- ¿Existen consideraciones sobre las auditorías de los sistemas?

3.6 Resultados de la encuesta a los colaboradores del departamento TI

A continuación, se muestra los resultados de la encuesta realizada al departamento TI en base a los Dominios de la Norma ISO 27002:

3.6.1 Resultados del dominio Política de seguridad

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Arquitectura TI
- Gerente de Mantenimiento de Sistemas
- Jefe de Seguridad de Información
- Director de Tecnología e Información

Existen documento(s) de políticas de seguridad de SI	☑ VERDADERO
Existe normativa relativa a la seguridad de los SI	☐ FALSO
Existen procedimientos relativos a la seguridad de SI	☑ VERDADERO
Existe un responsable de las políticas, normas y procedimientos	☑ VERDADERO
Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO
Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO

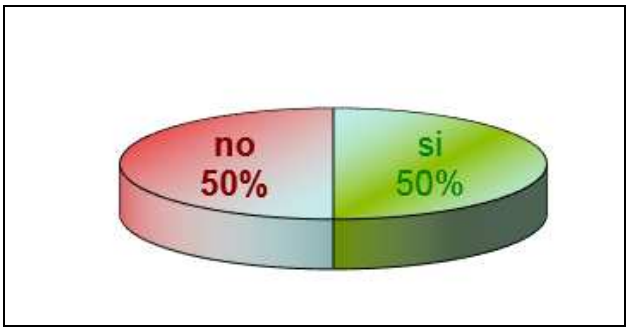


Figura 6 Resultado – Política de Seguridad

Resultados: De los encuestados, en un 50% se afirma que la Compañía tiene políticas, procedimientos o normativas relacionadas a Seguridad de Información, lo contrario, en un 50% se considera que la Compañía no dispone de esta documentación.

3.6.2 Resultados del dominio Aspectos de seguridad de la información

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Arquitectura TI
- Gerente de Mantenimiento de Sistemas
- Jefe de Seguridad de Información
- Director de Tecnología e Información

Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☑ VERDADERO
Existe un responsable encargado de evaluar la adquisición y cambios de SI	☑ VERDADERO
La Dirección y las áreas de la Organización participa en temas de seguridad	☑ VERDADERO
Existen condiciones contractuales de seguridad con terceros y outsourcing	☑ VERDADERO
Existen criterios de seguridad en el manejo de terceras partes	☑ VERDADERO
Existen programas de formación en seguridad para los empleados, clientes y terceros	☑ VERDADERO
Existe un acuerdo de confidencialidad de la información que se accesa.	☑ VERDADERO
Se revisa la organización de la seguridad periódicamente por una empresa externa	☐ FALSO

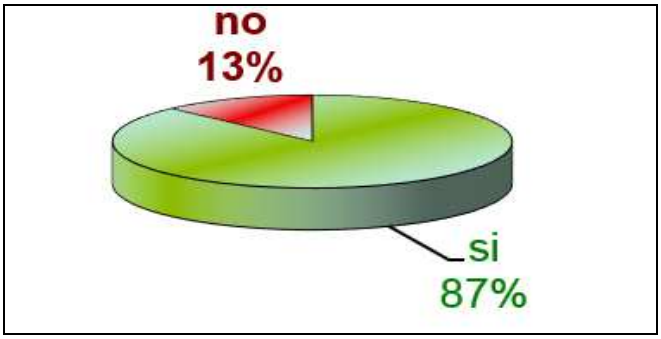


Figura 7 Resultado – Aspectos organizativos

Resultados: De los encuestados, en un 81% manifestó que, si se aplican los controles relacionados a este dominio, mientras que en un 13% se considera que no se han asignado responsabilidades para la seguridad de la información, ni en la gestión de proyectos y que no se aplican la mayoría de controles en este dominio.

3.6.3 Resultados del dominio Gestión de activos

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Jefe Regional de Soporte a Usuarios
- Gerente de Arquitectura TI
- Gerente de Mantenimiento de Sistemas
- Jefe de Seguridad de Información
- Director de Tecnología e Información

Existen un inventario de activos actualizado	☑ VERDADERO
El Inventario contiene activos de datos, software, equipos y servicios	☑ VERDADERO
Se dispone de una clasificación de la información según la criticidad de la misma	☑ VERDADERO
Existe un responsable de los activos	☑ VERDADERO
Existen procedimientos para clasificar la información	☑ VERDADERO
Existen procedimientos de etiquetado de la información	☐ FALSO

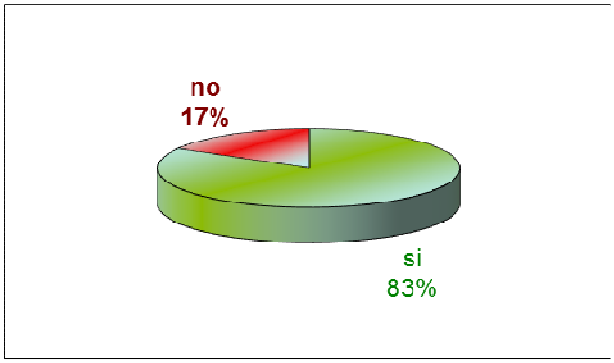


Figura 8 Resultado – Gestión de activos

Resultados: De los encuestados, en un 83% se determinó que el departamento TI tiene inventariado sus activos, de igual manera se ha clasificado la información y existe un adecuado manejo de soportes de almacenamiento, y en un 17% no se considera la existencia de estos controles.

3.6.4 Resultados del dominio Seguridad ligada a los recursos humanos

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Jefe de Seguridad de Información
- Director de Tecnología e Información

Se tienen definidas responsabilidades y roles de seguridad	☑ VERDADERO
Se tiene en cuenta la seguridad en la selección y baja del personal	☐ FALSO
Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☑ VERDADERO
Se imparte la formación adecuada de seguridad y tratamiento de activos	☐ FALSO
Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	☐ FALSO
Se recogen los datos de los incidentes de forma detallada	☑ VERDADERO
Informan los usuarios de las vulnerabilidades observadas o sospechadas	☑ VERDADERO
Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerab	☐ FALSO
Existe un proceso disciplinario de la seguridad de la información	☑ VERDADERO

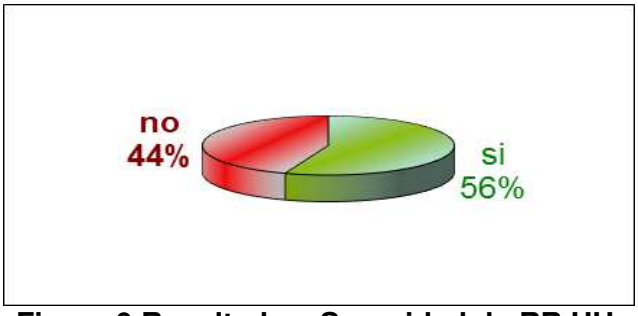


Figura 9 Resultado – Seguridad de RR.HH.

Resultados: De los encuestados, se considera que en un 56% existen controles antes, durante y después de la contratación de un colaborador. Mientras que en un 44%, no se considera la existencia de estos controles.

3.6.5 Resultados del dominio Seguridad física y ambiental

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Jefe de Seguridad de Información
- Jefe Regional de Soporte a Usuarios
- Gerente de Mantenimiento de Sistemas
- Director de Tecnología e Información

Existe perímetro de seguridad física(una pared, puerta con llave).	☑ VERDADERO
Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☑ VERDADERO
Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	☑ VERDADERO
En las áreas seguras existen controles adicionales al personal propio y ajeno	☑ VERDADERO
Las áreas de carga y expedición están aisladas de las áreas de SI	☑ VERDADERO
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	☑ VERDADERO
Existen protecciones frente a fallos en la alimentación eléctrica	☑ VERDADERO
Existe seguridad en el cableado frente a daños e intercepciones	☑ VERDADERO
Se asegura la disponibilidad e integridad de todos los equipos	☐ FALSO
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☐ FALSO
Se incluye la seguridad en equipos moviles	☐ FALSO

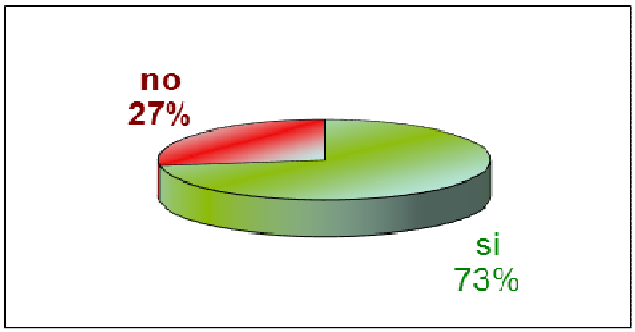


Figura 10 Resultado – Seguridad física

Resultados: En relación a este dominio, los encuestados consideraron que en un 73% se aplican controles relacionados a la seguridad perimetral, mientras que en un 27% se carece o existen debilidades de estos controles.

3.6.6 Resultados del dominio Seguridad en las operaciones

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Administradores de Aplicaciones
- Administradores de Bases de Datos
- Administrador de Redes

Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	FALSO
Estan establecidas responsabilidades para controlar los cambios en equipos	FALSO
Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	FALSO
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	FALSO
Existe una separación de los entornos de desarrollo y producción	VERDADERO
Existen contratistas externos para la gestión de los Sistemas de Información	VERDADERO
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	FALSO
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	FALSO
Controles contra software maligno	VERDADERO
Realizar copias de backup de la información esencial para el negocio	VERDADERO
Existen logs para las actividades realizadas por los operadores y administradores	FALSO
Existen logs de los fallos detectados	VERDADERO
Existen rastro de auditoría	FALSO
Existe algún control en las redes	VERDADERO
Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	FALSO
Eliminación de los medios informáticos. Pueden disponer de información sensible	FALSO
Existe seguridad de la documentación de los Sistemas	FALSO
Existen acuerdos para intercambio de información y software	VERDADERO
Existen medidas de seguridad de los medios en el tránsito	VERDADERO
Existen medidas de seguridad en el comercio electrónico.	FALSO
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	FALSO
Existen medidas de seguridad en las transacciones en linea	FALSO
Se monitorean las actividades relacionadas a la seguridad	VERDADERO

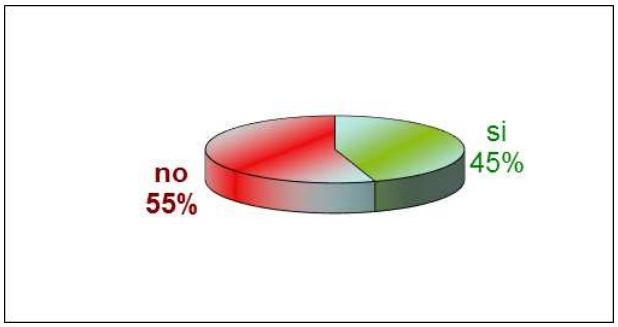


Figura 11 Resultado – Seguridad en las operaciones

Resultados: Los colaboradores encuestados consideran que en un 55% no se aplican los controles relacionados a seguridad a protección contra código malicioso, copias de seguridad, restricciones en instalación de software, entre otros. Por otro lado, en un 45% se considera que si se aplican controles para mitigar riesgos.

3.6.7 Resultados del dominio Control de accesos

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Administradores de Aplicaciones
- Administradores de Bases de Datos
- Administrador de Redes

Existe una política de control de accesos	☐ FALSO
Existe un procedimiento formal de registro y baja de accesos	☑ VERDADERO
Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	☐ FALSO
Existe una gestión de los password de usuarios	☑ VERDADERO
Existe una revisión de los derechos de acceso de los usuarios	☐ FALSO
Existe el uso del password	☑ VERDADERO
Se protege el acceso de los equipos desatendidos	☐ FALSO
Existen políticas de limpieza en el puesto de trabajo	☑ VERDADERO
Existe una política de uso de los servicios de red	☐ FALSO
Se asegura la ruta (path) desde el terminal al servicio	☑ VERDADERO
Existe una autenticación de usuarios en conexiones externas	☑ VERDADERO
Existe una autenticación de los nodos	☐ FALSO
Existe un control de la conexión de redes	☑ VERDADERO
Existe un control del routing de las redes	☑ VERDADERO
Existe una identificación única de usuario y una automática de terminales	☑ VERDADERO
Existen procedimientos de log-on al terminal	☐ FALSO
Se ha incorporado medidas de seguridad a la computación móvil	☐ FALSO
Está controlado el teletrabajo por la organización	☐ FALSO

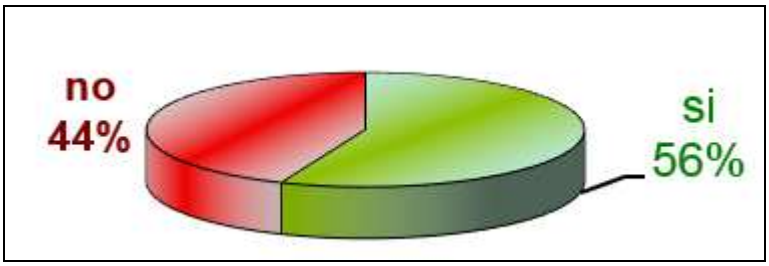


Figura 12 Resultado – Control de accesos

Resultados: De los encuestados, se considera que en un 56% existen un adecuado control de accesos a las redes, adicional se lleva una correcta gestión de altas y bajas de registros de colaboradores, además un correcto uso de herramientas para la administración de los sistemas. Sin embargo, en un 44% se considera que los controles asociados a este dominio no existen.

3.6.8 Resultados del dominio Mantenimiento de los sistemas

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Administradores de Aplicaciones

Se asegura que la seguridad está implantada en los Sistemas de Información	☐ FALSO
Existe seguridad en las aplicaciones	☑ VERDADERO
Existen controles criptográficos.	☐ FALSO
Existe seguridad en los ficheros de los sistemas	☐ FALSO
Existe seguridad en los procesos de desarrollo, testing y soporte	☐ FALSO
Existen controles de seguridad para los resultados de los sistemas	☐ FALSO
Existe la gestión de los cambios en los SO.	☑ VERDADERO
Se controlan las vulnerabilidades de los equipos	☐ FALSO

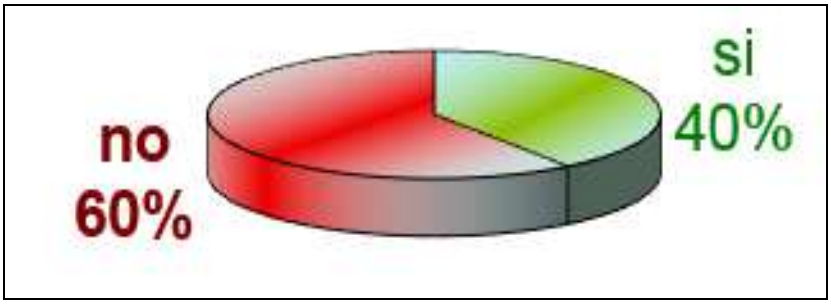


Figura 13 Resultado – Mantenimiento de los sistemas

Resultados: De los colaboradores encuestados, en un 60% se considera que el Departamento de TI no contempla controles relacionados a seguridades en los procesos de desarrollo de software tales como: pruebas de aceptación de usuario, aprobación de paso a producción entre otros. En un 40% se discurre que si existen los controles necesarios y que permita una adecuada seguridad de los sistemas de información.

3.6.9 Resultados del dominio Gestión de incidentes

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Gerente de Arquitectura TI
- Jefe de Seguridad de Información

Se comunican los eventos de seguridad	☑ VERDADERO
Se comunican las debilidades de seguridad	☑ VERDADERO
Existe definidas las responsabilidades antes un incidente.	☐ FALSO
Existe un procedimiento formal de respuesta	☐ FALSO
Existe la gestión de incidentes	☐ FALSO

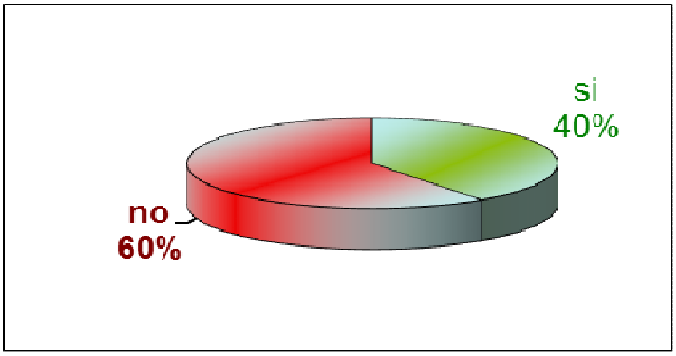


Figura 14 Resultado – Gestión de incidentes

Resultados: Para este dominio los colaboradores del área TI consideran que en un 60% no se llevan controles como: Responsabilidades y procedimientos en caso de un incidente, ni un adecuado manejo de respuestas, lo contrario en un 40% se considera que si existen controles relacionados.

3.6.10 Resultados del dominio Gestión de la continuidad del negocio

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Gerente de Arquitectura TI
- Jefe de Seguridad de Información
- Director de Tecnología e Información

Existen procesos para la gestión de la continuidad.	☐ FALSO
Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO
Existe un diseño, redacción e implantación de planes de continuidad	☐ FALSO
Existe un marco de planificación para la continuidad del negocio	☐ FALSO
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☐ FALSO

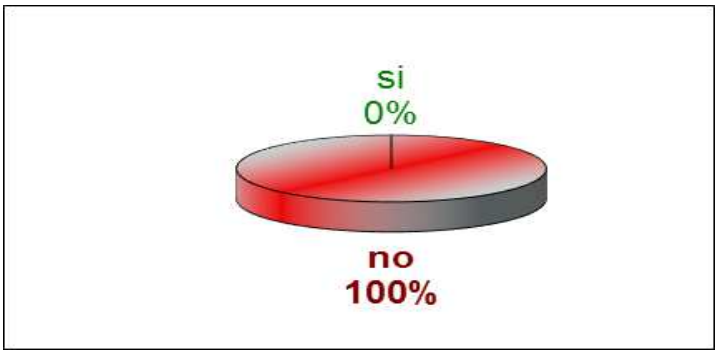


Figura 15 Resultado – Gestión de la continuidad del negocio

Resultados: De forma unánime se considera que no existen ningún control relacionado al dominio de continuidad de la seguridad de información.

3.6.11 Resultados del dominio Cumplimiento

De la encuesta realizada a los siguientes colaboradores del Departamento TI:

- Gerente de Mantenimiento de Sistemas
- Gerente de Arquitectura TI
- Jefe de Seguridad de Información
- Director de Tecnología e Información

Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☐ FALSO
Existe el resguardo de la propiedad intelectual	☑ VERDADERO
Existe el resguardo de los registros de la organización	☐ FALSO
Existe una revisión de la política de seguridad y de la conformidad técnica	☑ VERDADERO
Existen consideraciones sobre las auditorías de los sistemas	☑ VERDADERO

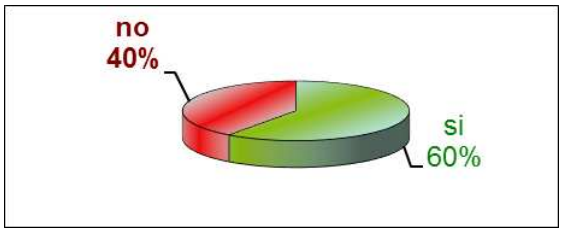


Figura 16 Resultado – Cumplimiento

Resultados: De los encuestados, en un 60% se considera que existe cumplimiento frente a requisitos legales y contractuales, así como derechos de propiedad intelectual entre otros controles; sin embargo, en un 40% se considera que no se aplica controles en este ámbito.

3.6.12 Resultados generales de la Norma ISO 27002

La figura 17, muestra que en un 62% se cumple con la mayoría de controles de los dominios de la Norma ISO y que en un 38% no se han aplicado los controles necesarios para fortalecer la Seguridad de Información de la Compañía:

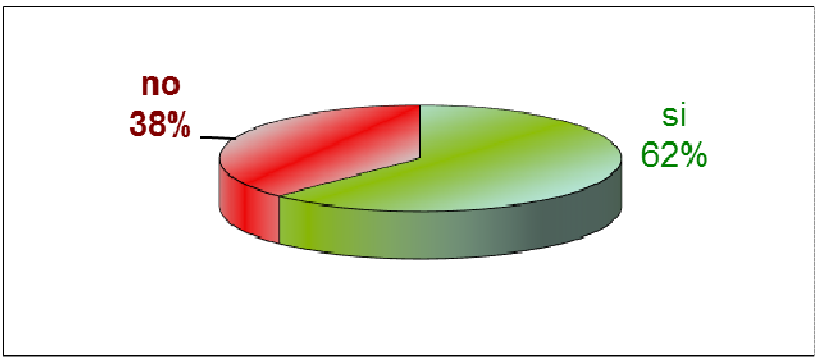


Figura 17 Resultados generales de la Norma ISO 27002

La evaluación realizada con los distintos Gerentes y Director de TI, ha permitido conocer la situación actual del departamento de Tecnología e Información en materia de Seguridad de Información y cumplimiento de los controles de la Norma ISO 270002.

3.7 Análisis de riesgos

A continuación, se aplica las fases de la metodología de análisis de riesgos en base a la metodología MAGERIT:

3.7.1 Identificación de activos de información

Como parte de la metodología se deben identificar los activos de información del Departamento de Tecnología e Información en base a:

[SW] Software: Se refiere a tareas automatizadas para el desempeño de la Organización.

Las aplicaciones permiten gestionar, analizar y transformar los datos permitiendo explotar la información para prestar distintos servicios (Amutio, 2012). A continuación, se detalla las aplicaciones relevantes que utiliza la Compañía:

3.7.2 Aplicaciones Informáticas

Posterior del análisis realizado con los Gerentes y Director TI se ha clasificado las aplicaciones críticas y sensibles para la Compañía y que deberán considerarse para el análisis de riesgos. La figura 18, muestra un mapa de calor de las aplicaciones relevantes para la operatividad de la Compañía:

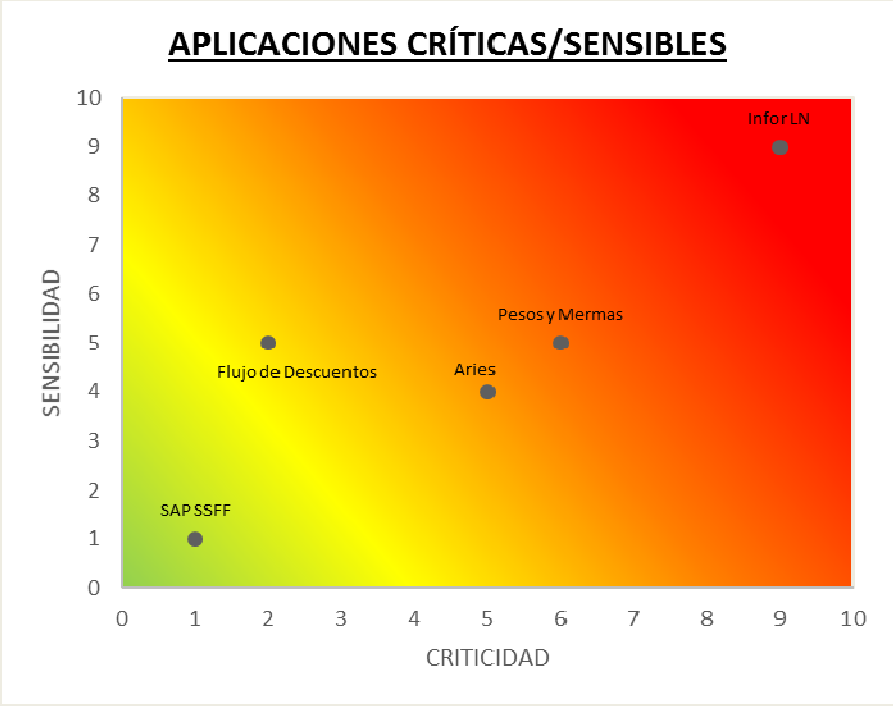


Figura 18 Mapa de Calor de aplicaciones críticas y sensibles

La aplicación relevante para la transaccionalidad de la Compañía es el ERP Infor LN el cual fue implementado en el año 2013. Cabe señalar que el ERP centraliza la mayoría de procesos relevantes de la Compañía, tales como: fórmulas de producción, estados financieros, control de calidad, planificación empresarial, entre otros.

Las demás aplicaciones: SAP SSFF, Flujo de descuentos, Pesos y mermas, Aries, se conectan al ERP y permite realizar la facturación de ventas de todas las marcas que maneja la Compañía, por ese motivo la aplicación relevante para el Departamento TI es: Infor LN y deberá realizarse el análisis de riesgos sobre este activo de información.

Parte del software que se maneja en la Compañía son las bases de datos y los sistemas operativos, a continuación se detalla el versionamiento y el tipo de BDD y SO utilizado:

3.7.3 Bases de Datos

El área de Tecnología cuenta con 65 licencias para uso de bases de datos Oracle distribuida en las siguientes versiones:

- Oracle Database 9.2 Enterprise Edition: 1
- Oracle Xpress 10g: 2
- Oracle 10g Enterprise Edition Release: 38
- Oracle Database 11g Enterprise Edition: 24

Además, se cuenta con bases de datos:

- SQL Server 2005
- SQL Server 2000
- SQL Server 2000 Standard
- SQL Server 2005 Express
- SQL Server 2005 Standard

3.7.4 Sistemas operativos

El área de Tecnología cuenta con los siguientes sistemas operativos:

- Sistema Operativo AIX: 5.3, 6.1, 7.1
- Red Hat Enterprise Linux 4, 5 y 7
- Windows Server 2003, 2005, 2008, 2012

[HW] Equipamiento informático: Son los medios materiales o físicos que permiten dan soporte a los servicios que presta la Compañía, siendo equipamiento temporal o permanente de los datos.

A continuación, se cita el equipamiento relevante para las operaciones de la Organización:

3.7.5 Cintas de respaldos

Los respaldos de las bases de datos se lo realizan mediante la solución TSM – IBM, la información respaldada son de los aplicativos:

- Infor LN
- BAAN 4
- BAAN 5

Se ubican en el Edificio Inverna y se tienen 400 cintas para backups.

3.7.6 Almacenamiento

Para el almacenamiento se cuenta con soluciones FTP SAP y Filenet, la ubicación es mediante un servicio en la nube de Microsoft Azure e IBM Softlayer.

3.7.7 Servidores

La Compañía contempla 13 servidores físicos distribuidos en Quito (9 servidores), Guayaquil (1 servidor), IBM (2 servidores), Telconet (1 servidor).

3.7.8 Equipamiento en centro de datos

El centro de datos cuenta con los siguientes elementos:

- 3 AC marca Liebert
- 1 UPS marca APC
- 1 UPS marca Liebert
- 1 sistema de monitoreo Blue Box
- 1 Sistema contra incendios

- 1 PDU eléctrico
- 2 bombonas de gas FM200
- 1 cámara de seguridad
- 1 Switch 4503
- 2 Switch Nexus

3.8 Ingreso de activos de información a la herramienta PILAR

Después de haber identificado los activos principales del área tecnológica, se deben ingresar en la herramienta para conocer las principales vulnerabilidades de los activos y cuáles son las amenazas que podrían explotar dichas vulnerabilidades y con ello identificar riesgos con la finalidad de establecer medidas preventivas y correctivas.

En primera instancia se deben llenar los datos para generar un archivo, como se muestra en la figura 19:

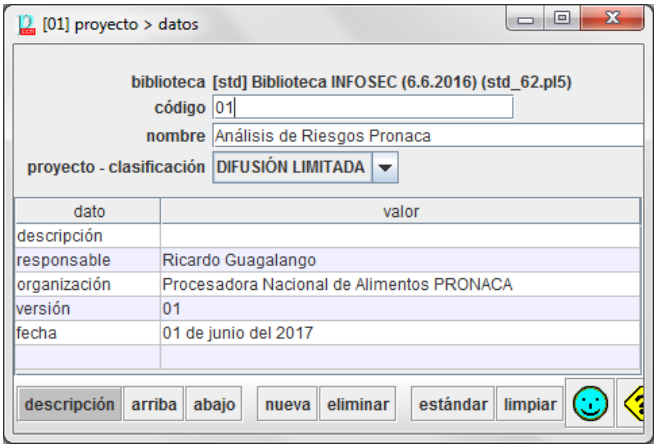


Figura 19 Interfaz de creación de proyecto.

Como se muestra en la figura 20, se debe ingresar los activos relevantes identificados con el personal de TI en la herramienta PILAR:

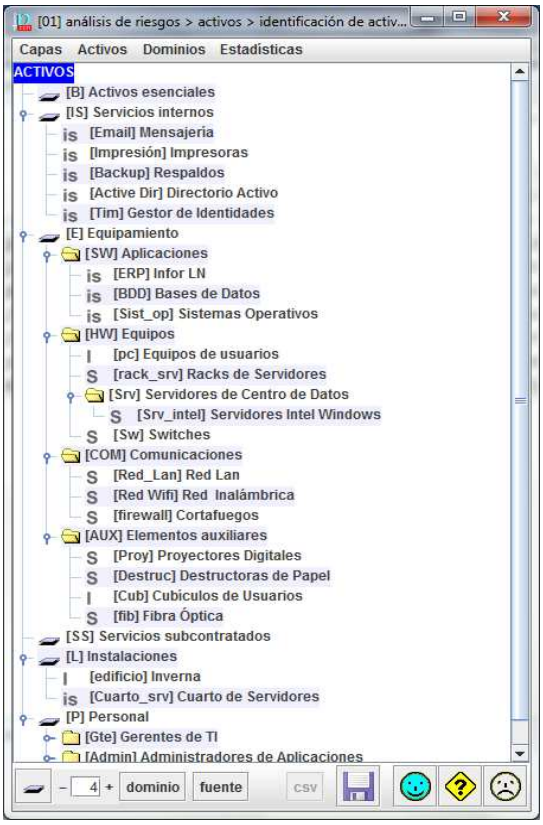


Figura 20 Identificación de activos

3.9 Valoración de activos

En la herramienta PILAR se debe valorar con base a las siguientes dimensiones. Según (Amutio, 2012) define:

- [D] Disponibilidad: Asegura que los colaboradores autorizados tienen acceso a la información y activos cuando estos lo requieran.
- [I] Integridad: Garantiza que los datos e información no ha sido modificada ni eliminada sin autorización.
- [C] Confidencialidad: Asegura el acceso a la información a las personas autorizadas.
- [A] Autenticidad: Identifica el usuario que genera la información y no la suplantación de identidad.

- [T] Trazabilidad: Asegura de que en todo momento se podrá determinar quién hizo qué y en qué momento ciertas acciones.
- [V] Valoración: Los activos son valorados para establecer requisitos de seguridad.

Para los activos de información, se valora el nivel requerido de seguridad con respecto a la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad en base a los siguientes criterios de valoración que la herramienta PILAR proporciona acorde a la metodología MAGERIT:

Tabla 16
Criterios de valoración

Valor	Nivel	Criterio
n.a.	No aplica	-
[0]	Despreciable	Irrelevante a efectos prácticos
[1]	Bajo	Daño menor
[2]	Bajo (+)	Daño menor
[3]	Medio (-)	Daño importante
[4]	Medio	Daño importante
[5]	Medio (+)	Daño importante
[6]	Alto (-)	Daño grave
[7]	Alto	Daño grave
[8]	Alto (+)	Daño grave
[9]	Muy Alto	Daño muy grave
[10]	Extremo	Daño extremadamente grave

La figura 21, muestra cómo se valoran los activos por cada activo de información identificado:

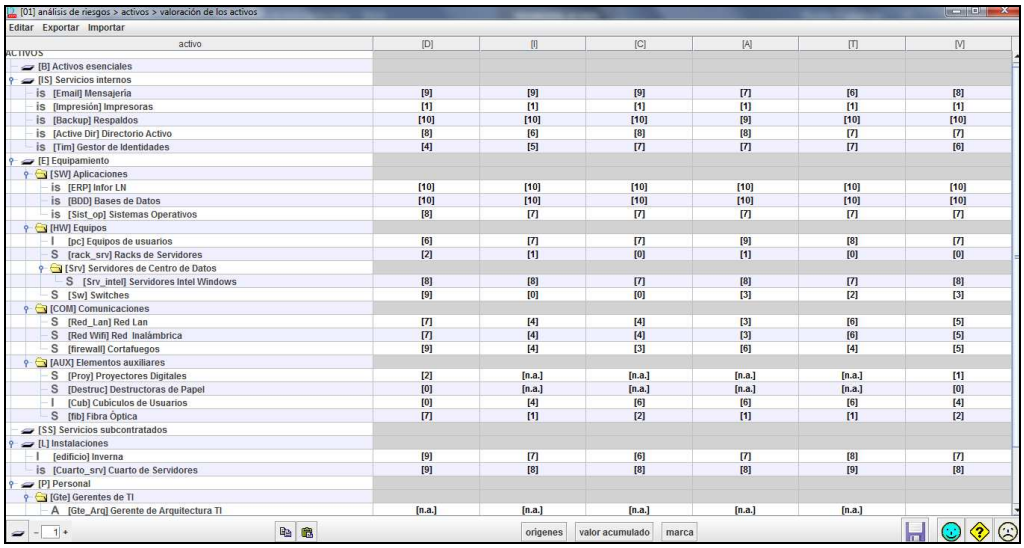


Figura 21 Valoración de activos

Los activos son valorados de acuerdo a los cinco criterios, a continuación el detalle de cada activo de información valorado:

capa: [IS] Servicios internos

Activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[V]**
[Email] Mensajería	[9]	[9]	[9]	[7]	[6]	[8]
[Impresión] Impresoras	[1]	[1]	[1]	[1]	[1]	[1]
[Backup] Respaldos	[10]	[10]	[10]	[9]	[10]	[10]
[Active Dir] Directorio Activo	[8]	[6]	[8]	[8]	[7]	[7]
[Tim] Gestor de Identidades	[4]	[5]	[7]	[7]	[7]	[6]

capa: [E] Equipamiento

Activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[V]**
[ERP] Infor LN	[10]	[10]	[10]	[10]	[10]	[10]
[BDD] Bases de Datos	[10]	[10]	[10]	[10]	[10]	[10]
[Sist_op] Sistemas Operativos	[8]	[7]	[7]	[7]	[7]	[7]
[pc] Equipos de usuarios	[6]	[7]	[7]	[9]	[8]	[7]
[rack_srv] Racks de Servidores	[2]	[1]	[0]	[1]	[0]	[0]
[Srv_intel] Servidores Intel Windows	[8]	[8]	[7]	[8]	[7]	[8]
[Sw] Switches	[9]	[0]	[0]	[3]	[2]	[3]
[Red_Lan] Red Lan	[7]	[4]	[4]	[3]	[6]	[5]
[Red Wifi] Red Inalámbrica	[7]	[4]	[4]	[3]	[6]	[5]
[firewall] Cortafuegos	[9]	[4]	[3]	[6]	[4]	[5]
[Proy] Proyectores Digitales	[2]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[1]
[Destruc] Destructoras de Papel	[0]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[0]
[Cub] Cubículos de Usuarios	[0]	[4]	[6]	[6]	[6]	[4]
[fib] Fibra Óptica	[7]	[1]	[2]	[1]	[1]	[2]

capa: [L] Instalaciones

activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[V]**
[edificio] Inverna	[9]	[7]	[6]	[7]	[8]	[7]
[Cuarto_srv] Cuarto de Servidores	[9]	[8]	[8]	[8]	[9]	[8]

La figura 22, muestra en modo gráfico la identificación y valoración de activos que proporciona la herramienta PILAR:

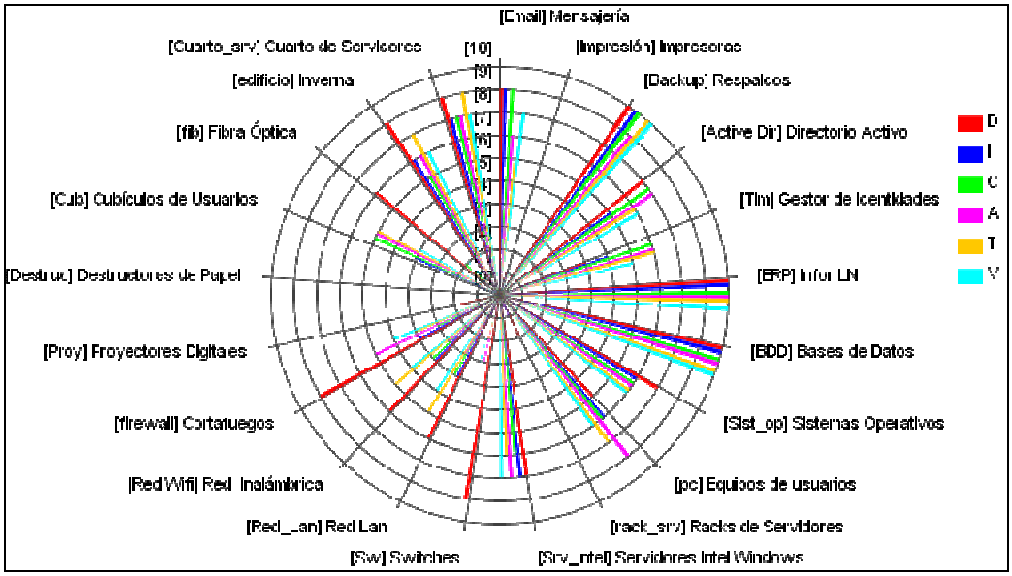


Figura 22 Identificación y valoración de activos

Se identifica que dos activos de información se verían afectados en: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad si amenazas se materializarían en riesgos causando daños potenciales a la transaccionalidad de las operaciones de la Compañía, siendo los siguientes:

- ERP Infor LN
- Bases de Datos

3.10 Identificación de amenazas

En esta fase se identifica las amenazas que tienen posibilidad de causar afectación sobre los activos de información. La herramienta PILAR posee una biblioteca de amenazas y estas se asocian a cada uno de los activos.

La figura 23, muestra el catálogo de amenazas que proporciona PILAR por cada activo de información:

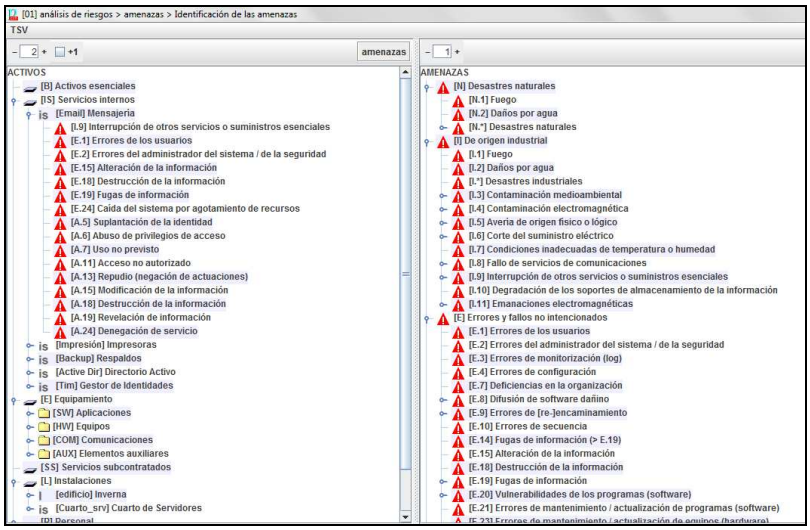


Figura 23 Identificación de amenazas

A continuación, se muestra el detalle de las amenazas identificadas y porcentajes de afectación sobre cada parámetro: disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad. También, la frecuencia que causaría dicha amenaza por cada activo de información:

[Email] Mensajería

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-

[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	1	-	-	-	-	-

[Impresión] Impresoras

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.9] Interrupción de otros servicios o suministros esenciales	1	5%	-	-	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	10	-	10%	50%	-	-
[A.11] Acceso no autorizado	100	-	10%	50%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	1	5%	-	-	-	-

[Backup] Respaldos

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.3] Errores de monitorización (log)	1	-	1%	-	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.3] Manipulación de los registros de actividad (log)	100	-	50%	-	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	1	-	-	-	-	-

[Active Dir] Directorio Activo

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.5] Suplantación de la identidad	1	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	5	-	-	-	-	100%
[A.15] Modificación de la información	10	-	50%	-	-	-

[A.18] Destrucción de la información	1	-	-	-	-	-
[A.24] Denegación de servicio	10	-	-	-	-	-

[Tim] Gestor de Identidades

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	20%	20%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	5%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	5	-	-	-	-	100%
[A.15] Modificación de la información	10	-	50%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.24] Denegación de servicio	10	5%	-	-	-	-

[ERP] Infor LN

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.3] Errores de monitorización (log)	1	-	1%	-	-	-
[E.8] Difusión de software dañino	1	-	10%	10%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	-	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	1%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.3] Manipulación de los registros de actividad (log)	100	-	50%	-	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.8] Difusión de software dañino	1	-	100%	100%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	-	100%	100%	-	-
[A.24] Denegación de servicio	1	-	-	-	-	-

[BDD] Bases de Datos

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.3] Errores de monitorización (log)	1	-	1%	-	-	-
[E.8] Difusión de software dañino	1	-	10%	10%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-

[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	-	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	1%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.3] Manipulación de los registros de actividad (log)	100	-	50%	-	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.8] Difusión de software dañino	1	-	100%	100%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	-	100%	100%	-	-
[A.24] Denegación de servicio	1	-	-	-	-	-

[Sist_op] Sistemas Operativos

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.8] Difusión de software dañino	1	-	10%	10%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	-	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	1%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	10%	10%	-	-
[A.8] Difusión de software dañino	1	-	100%	100%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	-	100%	100%	-	-
[A.24] Denegación de servicio	1	-	-	-	-	-

[pc] Equipos de usuarios

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	10%	-	-	-	-
[N.2] Daños por agua	0,1	5%	-	-	-	-
[N.*] Desastres naturales	0,1	10%	-	-	-	-
[I.1] Fuego	0,5	10%	-	-	-	-
[I.2] Daños por agua	0,5	5%	-	-	-	-
[I.*] Desastres industriales	0,5	10%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	5%	-	-	-	-
[I.4] Contaminación electromagnética	1	1%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	5%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	10%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	10%	-	-	-	-
[I.9] Interrupción de otros servicios o	1	5%	-	-	-	-

suministros esenciales						
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	20%	20%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	5%	-	-	-	-
[E.25] Pérdida de equipos	5	1%	-	10%	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	1%	1%	10%	-	-
[A.11] Acceso no autorizado	1	1%	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.23] Manipulación del hardware	0,5	5%	-	50%	-	-
[A.24] Denegación de servicio	2	10%	-	-	-	-
[A.25] Robo de equipos	5	1%	-	10%	-	-
[A.26] Ataque destructivo	1	10%	-	-	-	-

[rack_srv] Racks de Servidores

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	1	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	10%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	100%	-	100%	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	-	-
[A.7] Uso no previsto	1	10%	10%	100%	-	-
[A.11] Acceso no autorizado	1	10%	100%	100%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	2	100%	-	-	-	-
[A.25] Robo de equipos	0,1	100%	-	100%	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

[Srv_intel] Servidores Intel Windows

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	-	-	-	-	-
[N.2] Daños por agua	0,1	-	-	-	-	-
[N.*] Desastres naturales	0,1	-	-	-	-	-
[I.1] Fuego	0,5	-	-	-	-	-
[I.2] Daños por agua	0,5	-	-	-	-	-
[I.*] Desastres industriales	0,5	-	-	-	-	-
[I.3] Contaminación medioambiental	0,1	-	-	-	-	-
[I.4] Contaminación electromagnética	1	-	-	-	-	-
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.6] Corte del suministro eléctrico	1	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[E.25] Pérdida de equipos	1	-	-	100%	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	100%	100%	100%	-
[A.7] Uso no previsto	1	-	10%	100%	-	-
[A.11] Acceso no autorizado	1	-	100%	100%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	2	-	-	-	-	-
[A.25] Robo de equipos	0,1	-	-	100%	-	-
[A.26] Ataque destructivo	1	-	-	-	-	-

[Sw] Switches

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	-	-	-	-	-
[N.2] Daños por agua	0,1	-	-	-	-	-
[N.*] Desastres naturales	0,1	-	-	-	-	-
[I.1] Fuego	0,5	-	-	-	-	-
[I.2] Daños por agua	0,5	-	-	-	-	-
[I.*] Desastres industriales	0,5	-	-	-	-	-
[I.3] Contaminación medioambiental	0,1	-	-	-	-	-
[I.4] Contaminación electromagnética	1	-	-	-	-	-
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.6] Corte del suministro eléctrico	1	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[E.25] Pérdida de equipos	1	-	-	100%	-	-
[A.7] Uso no previsto	1	-	1%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	-	-
[A.23] Manipulación del hardware	0,5	-	-	50%	-	-
[A.24] Denegación de servicio	2	-	-	-	-	-
[A.25] Robo de equipos	0,1	-	-	100%	-	-
[A.26] Ataque destructivo	1	-	-	-	-	-

[Red_Lan] Red Lan

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	5%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	5%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.14] Interceptación de información (escucha)	1	-	-	1%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	5%	-	-	-	-

[Red Wifi] Red Inalámbrica

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	5%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	5%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	5%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.14] Interceptación de información (escucha)	1	-	-	5%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	5%	-	-	-	-

[firewall] Cortafuegos

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	5%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	20%	20%	-	-
[E.4] Errores de configuración	1	-	1%	-	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-

[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	5%	-	-	-	-
[A.4] Manipulación de los ficheros de configuración	10	1%	10%	10%	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.14] Interceptación de información (escucha)	1	-	-	10%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	5%	-	-	-	-

[Proy] Proyectores Digitales

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	10%	-	-	-	-
[N.2] Daños por agua	0,1	5%	-	-	-	-
[N.*] Desastres naturales	0,1	10%	-	-	-	-
[I.1] Fuego	0,5	10%	-	-	-	-
[I.2] Daños por agua	0,5	5%	-	-	-	-
[I.*] Desastres industriales	0,5	10%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	5%	-	-	-	-
[I.4] Contaminación electromagnética	1	1%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	5%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	10%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	10%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	-	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	5%	-	-	-	-
[E.25] Pérdida de equipos	1	10%	-	-	-	-
[A.6] Abuso de privilegios de acceso	1	-	-	-	-	-
[A.7] Uso no previsto	1	5%	-	-	-	-
[A.11] Acceso no autorizado	1	1%	-	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.23] Manipulación del hardware	1	5%	-	-	-	-
[A.24] Denegación de servicio	2	10%	-	-	-	-
[A.25] Robo de equipos	0,5	1%	-	-	-	-
[A.26] Ataque destructivo	1	1%	-	-	-	-

[Destruc] Destructoras de Papel

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	-	-	-	-	-
[N.2] Daños por agua	0,1	-	-	-	-	-
[N.*] Desastres naturales	0,1	-	-	-	-	-
[I.1] Fuego	0,5	-	-	-	-	-
[I.2] Daños por agua	0,5	-	-	-	-	-
[I.*] Desastres industriales	0,5	-	-	-	-	-
[I.3] Contaminación medioambiental	0,1	-	-	-	-	-
[E.1] Errores de los usuarios	1	1%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	2%	-	-	-	-
[E.18] Destrucción de la información	1	1%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	5%	-	-	-	-
[A.6] Abuso de privilegios de acceso	1	-	-	-	-	-

[A.7] Uso no previsto	1	-	-	-	-	-
[A.18] Destrucción de la información	1	5%	-	-	-	-
[A.23] Manipulación del hardware	1	-	-	-	-	-
[A.24] Denegación de servicio	10	5%	-	-	-	-

[Cub] Cubículos de Usuarios

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	10%	-	-	-	-
[N.2] Daños por agua	0,1	5%	-	-	-	-
[N.*] Desastres naturales	0,1	10%	-	-	-	-
[I.1] Fuego	0,5	10%	-	-	-	-
[I.2] Daños por agua	0,5	5%	-	-	-	-
[I.*] Desastres industriales	0,5	10%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	5%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1%	-	-	-	-
[A.7] Uso no previsto	1	5%	1%	1%	-	-
[A.23] Manipulación del hardware	1	5%	-	50%	-	-
[A.25] Robo de equipos	0,5	1%	-	50%	-	-
[A.26] Ataque destructivo	1	1%	-	-	-	-

[fib] Fibra Óptica

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	-	-	-	-	-
[N.2] Daños por agua	0,1	-	-	-	-	-
[N.*] Desastres naturales	0,1	-	-	-	-	-
[I.1] Fuego	0,5	-	-	-	-	-
[I.2] Daños por agua	0,5	-	-	-	-	-
[I.*] Desastres industriales	0,5	-	-	-	-	-
[I.3] Contaminación medioambiental	0,1	-	-	-	-	-
[I.8] Fallo de servicios de comunicaciones	1	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	-	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.7] Uso no previsto	1	-	1%	1%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.14] Interceptación de información (escucha)	1	-	-	5%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.23] Manipulación del hardware	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	-	-	-	-	-
[A.25] Robo de equipos	0,8	-	-	-	-	-
[A.26] Ataque destructivo	1	-	-	-	-	-

[edificio] Inverna

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	1	-	-	-	-	-
[N.2] Daños por agua	1	-	-	-	-	-
[N.*] Desastres naturales	0,5	-	-	-	-	-
[I.1] Fuego	1	-	-	-	-	-
[I.2] Daños por agua	1	-	-	-	-	-
[I.*] Desastres industriales	1	-	-	-	-	-
[I.3] Contaminación	1	-	-	-	-	-

medioambiental						
[I.4] Contaminación electromagnética	0,1	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	1	-	-	-	-	-
[A.7] Uso no previsto	1	-	-	-	-	-
[A.26] Ataque destructivo	0,1	-	-	-	-	-
[A.27] Ocupación enemiga	1	-	-	-	-	-

[Cuarto_srv] Cuarto de Servidores

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	1	-	-	-	-	-
[N.2] Daños por agua	1	-	-	-	-	-
[N.*] Desastres naturales	0,5	-	-	-	-	-
[I.1] Fuego	1	-	-	-	-	-
[I.2] Daños por agua	1	-	-	-	-	-
[I.*] Desastres industriales	1	-	-	-	-	-
[I.3] Contaminación medioambiental	1	-	-	-	-	-
[I.4] Contaminación electromagnética	0,1	-	-	-	-	-
[I.5] Avería de origen físico o lógico	1	-	-	-	-	-
[I.6] Corte del suministro eléctrico	1	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.1] Errores de los usuarios	1	-	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	-	20%	20%	-	-
[E.15] Alteración de la información	1	-	10%	-	-	-
[E.18] Destrucción de la información	1	-	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	-	-	-	-	-
[E.25] Pérdida de equipos	0,1	-	-	100%	-	-
[A.5] Suplantación de la identidad	0,2	-	100%	100%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	10%	100%	-
[A.7] Uso no previsto	1	-	1%	10%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	1	-	-	-	-	100%
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	-	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.23] Manipulación del hardware	0,5	-	-	50%	-	-
[A.24] Denegación de servicio	2	-	-	-	-	-
[A.25] Robo de equipos	0,1	-	-	100%	-	-
[A.26] Ataque destructivo	0,1	-	-	-	-	-
[A.27] Ocupación enemiga	1	-	-	-	-	-

A continuación, se muestra el detalle de los activos y porcentajes de afectación sobre cada parámetro: disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad. De igual manera, la frecuencia que causaría dicha amenaza por cada activo de información:

[N.1] Fuego

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,1	10%	-	-	-	-
[rack_srv] Racks de Servidores	0,1	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,1	-	-	-	-	-
[Sw] Switches	0,1	-	-	-	-	-
[Proy] Proyectores Digitales	0,1	10%	-	-	-	-
[Destruc] Destructoras de Papel	0,1	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,1	10%	-	-	-	-
[fib] Fibra Óptica	0,1	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[N.2] Daños por agua

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,1	5%	-	-	-	-
[rack_srv] Racks de Servidores	0,1	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,1	-	-	-	-	-
[Sw] Switches	0,1	-	-	-	-	-
[Proy] Proyectores Digitales	0,1	5%	-	-	-	-
[Destruc] Destructoras de Papel	0,1	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,1	5%	-	-	-	-
[fib] Fibra Óptica	0,1	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[N.*] Desastres naturales

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,1	10%	-	-	-	-
[rack_srv] Racks de Servidores	0,1	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,1	-	-	-	-	-
[Sw] Switches	0,1	-	-	-	-	-
[Proy] Proyectores Digitales	0,1	10%	-	-	-	-
[Destruc] Destructoras de Papel	0,1	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,1	10%	-	-	-	-
[fib] Fibra Óptica	0,1	-	-	-	-	-
[edificio] Inverna	0,5	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	0,5	-	-	-	-	-

[I.1] Fuego

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,5	10%	-	-	-	-
[rack_srv] Racks de Servidores	0,5	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,5	-	-	-	-	-
[Sw] Switches	0,5	-	-	-	-	-
[Proy] Proyectores Digitales	0,5	10%	-	-	-	-

[Destruc] Destructoras de Papel	0,5	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,5	10%	-	-	-	-
[fib] Fibra Óptica	0,5	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.2] Daños por agua

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,5	5%	-	-	-	-
[rack_srv] Racks de Servidores	0,5	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,5	-	-	-	-	-
[Sw] Switches	0,5	-	-	-	-	-
[Proy] Proyectores Digitales	0,5	5%	-	-	-	-
[Destruc] Destructoras de Papel	0,5	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,5	5%	-	-	-	-
[fib] Fibra Óptica	0,5	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.*] Desastres industriales

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,5	10%	-	-	-	-
[rack_srv] Racks de Servidores	0,5	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,5	-	-	-	-	-
[Sw] Switches	0,5	-	-	-	-	-
[Proy] Proyectores Digitales	0,5	10%	-	-	-	-
[Destruc] Destructoras de Papel	0,5	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,5	10%	-	-	-	-
[fib] Fibra Óptica	0,5	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.3] Contaminación medioambiental

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,1	5%	-	-	-	-
[rack_srv] Racks de Servidores	0,1	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	0,1	-	-	-	-	-
[Sw] Switches	0,1	-	-	-	-	-
[Proy] Proyectores Digitales	0,1	5%	-	-	-	-
[Destruc] Destructoras de Papel	0,1	-	-	-	-	-
[Cub] Cubículos de Usuarios	0,1	5%	-	-	-	-
[fib] Fibra Óptica	0,1	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.4] Contaminación electromagnética

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	1%	-	-	-	-
[rack_srv] Racks de Servidores	1	10%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[edificio] Inverna	0,1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	0,1	-	-	-	-	-

[I.5] Avería de origen físico o lógico

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	1	-	-	-	-	-
[BDD] Bases de Datos	1	-	-	-	-	-
[Sist_op] Sistemas Operativos	1	-	-	-	-	-
[pc] Equipos de usuarios	1	5%	-	-	-	-
[rack_srv] Racks de Servidores	1	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	5%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.6] Corte del suministro eléctrico

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	10%	-	-	-	-
[rack_srv] Racks de Servidores	1	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	10%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.7] Condiciones inadecuadas de temperatura o humedad

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	10%	-	-	-	-
[rack_srv] Racks de Servidores	1	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	10%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.8] Fallo de servicios de comunicaciones

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	5%	-	-	-	-
[Red Wifi] Red Inalámbrica	1	5%	-	-	-	-
[firewall] Cortafuegos	1	5%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-

[I.9] Interrupción de otros servicios o suministros esenciales

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	-	-	-
[Impresión] Impresoras Lexmark	1	5%	-	-	-	-
[Backup] Respaldos	1	-	-	-	-	-
[ERP] Infor LN	1	-	-	-	-	-
[BDD] Bases de Datos	1	-	-	-	-	-
[Sist_op] Sistemas Operativos	1	-	-	-	-	-
[pc] Equipos de usuarios	1	5%	-	-	-	-
[rack_srv] Racks de Servidores	1	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Red Wifi] Red Inalámbrica	1	5%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[I.11] Emanaciones electromagnéticas

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	-	-	1%	-	-
[rack_srv] Racks de Servidores	1	-	-	1%	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	1%	-	-
[Sw] Switches	1	-	-	1%	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	1%	-	-

[E.1] Errores de los usuarios

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	10%	10%	-	-
[Backup] Respaldos	1	-	10%	10%	-	-
[Active Dir] Directorio Activo	1	-	10%	10%	-	-
[Tim] Gestor de Identidades	1	1%	10%	10%	-	-
[ERP] Infor LN	1	-	10%	10%	-	-
[BDD] Bases de Datos	1	-	10%	10%	-	-
[Sist_op] Sistemas Operativos	1	-	10%	10%	-	-
[pc] Equipos de usuarios	1	1%	10%	10%	-	-
[Srv_intel] Servidores Intel Windows	1	-	10%	10%	-	-
[Red_Lan] Red Lan	1	1%	10%	10%	-	-
[Red Wifi] Red Inalámbrica	1	1%	10%	10%	-	-
[firewall] Cortafuegos	1	1%	10%	10%	-	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[Destruc] Destructoras de Papel	1	1%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	10%	10%	-	-

[E.2] Errores del administrador del sistema / de la seguridad

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	20%	20%	-	-
[Backup] Respaldos	1	-	20%	20%	-	-
[Active Dir] Directorio Activo	1	-	20%	20%	-	-
[Tim] Gestor de Identidades	1	2%	20%	20%	-	-
[ERP] Infor LN	1	-	20%	20%	-	-
[BDD] Bases de Datos	1	-	20%	20%	-	-

[Sist_op] Sistemas Operativos	1	-	20%	20%	-	-
[pc] Equipos de usuarios	1	2%	20%	20%	-	-
[Srv_intel] Servidores Intel Windows	1	-	20%	20%	-	-
[Red_Lan] Red Lan	1	2%	20%	20%	-	-
[Red Wifi] Red Inalámbrica	1	2%	20%	20%	-	-
[firewall] Cortafuegos	1	2%	20%	20%	-	-
[Proy] Proyectores Digitales	1	2%	-	-	-	-
[Destruc] Destructoras de Papel	1	2%	-	-	-	-
[fib] Fibra Óptica	1	-	20%	20%	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	20%	20%	-	-

[E.3] Errores de monitorización (log)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Backup] Respaldos	1	-	1%	-	-	-
[ERP] Infor LN	1	-	1%	-	-	-
[BDD] Bases de Datos	1	-	1%	-	-	-

[E.4] Errores de configuración

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[firewall] Cortafuegos	1	-	1%	-	-	-

[E.8] Difusión de software dañino

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	1	-	10%	10%	-	-
[BDD] Bases de Datos	1	-	10%	10%	-	-
[Sist_op] Sistemas Operativos	1	-	10%	10%	-	-

[E.9] Errores de [re-]encaminamiento

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	-	10%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	10%	-	-
[firewall] Cortafuegos	1	-	-	10%	-	-
[fib] Fibra Óptica	1	-	-	10%	-	-

[E.10] Errores de secuencia

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	10%	-	-	-
[Red Wifi] Red Inalámbrica	1	-	10%	-	-	-
[firewall] Cortafuegos	1	-	10%	-	-	-
[fib] Fibra Óptica	1	-	10%	-	-	-

[E.15] Alteración de la información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	10%	-	-	-
[Impresión] Impresoras Lexmark	1	-	10%	-	-	-

[Backup] Respaldos	1	-	10%	-	-	-
[Active Dir] Directorio Activo	1	-	1%	-	-	-
[Tim] Gestor de Identidades	1	-	1%	-	-	-
[ERP] Infor LN	1	-	10%	-	-	-
[BDD] Bases de Datos	1	-	10%	-	-	-
[Sist_op] Sistemas Operativos	1	-	10%	-	-	-
[pc] Equipos de usuarios	1	-	10%	-	-	-
[rack_srv] Racks de Servidores	1	-	10%	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	10%	-	-	-
[Red_Lan] Red Lan	1	-	1%	-	-	-
[Red Wifi] Red Inalámbrica	1	-	1%	-	-	-
[firewall] Cortafuegos	1	-	1%	-	-	-
[fib] Fibra Óptica	1	-	1%	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	10%	-	-	-

[E.18] Destrucción de la información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	-	-	-
[Impresión] Impresoras Lexmark	1	1%	-	-	-	-
[Backup] Respaldos	1	-	-	-	-	-
[Active Dir] Directorio Activo	1	-	-	-	-	-
[Tim] Gestor de Identidades	1	1%	-	-	-	-
[ERP] Infor LN	1	-	-	-	-	-
[BDD] Bases de Datos	1	-	-	-	-	-
[Sist_op] Sistemas Operativos	1	-	-	-	-	-
[pc] Equipos de usuarios	1	1%	-	-	-	-
[rack_srv] Racks de Servidores	1	10%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Red_Lan] Red Lan	1	1%	-	-	-	-
[Red Wifi] Red Inalámbrica	1	1%	-	-	-	-
[firewall] Cortafuegos	1	1%	-	-	-	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[Destruc] Destructoras de Papel	1	1%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[E.19] Fugas de información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	10%	-	-
[Impresión] Impresoras Lexmark	1	-	-	10%	-	-
[Backup] Respaldos	1	-	-	10%	-	-
[Active Dir] Directorio Activo	1	-	-	10%	-	-
[Tim] Gestor de Identidades	1	-	-	10%	-	-
[ERP] Infor LN	1	-	-	10%	-	-
[BDD] Bases de Datos	1	-	-	10%	-	-
[Sist_op] Sistemas Operativos	1	-	-	10%	-	-
[pc] Equipos de usuarios	1	-	-	10%	-	-
[rack_srv] Racks de Servidores	1	-	-	10%	-	-
[Srv_intel] Servidores Intel	1	-	-	10%	-	-

Windows						
[Red_Lan] Red Lan	1	-	-	10%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	10%	-	-
[firewall] Cortafuegos	1	-	-	10%	-	-
[fib] Fibra Óptica	1	-	-	10%	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	10%	-	-

[E.20] Vulnerabilidades de los programas (software)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	1	-	20%	20%	-	-
[BDD] Bases de Datos	1	-	20%	20%	-	-
[Sist_op] Sistemas Operativos	1	-	20%	20%	-	-

[E.21] Errores de mantenimiento / actualización de programas (software)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	10	-	1%	-	-	-
[BDD] Bases de Datos	10	-	1%	-	-	-
[Sist_op] Sistemas Operativos	10	-	1%	-	-	-

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	1%	-	-	-	-
[rack_srv] Racks de Servidores	1	10%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[Destruc] Destructoras de Papel	1	-	-	-	-	-
[Cub] Cubículos de Usuarios	1	1%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[E.24] Caída del sistema por agotamiento de recursos

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	10	-	-	-	-	-
[Backup] Respaldos	10	-	-	-	-	-
[Active Dir] Directorio Activo	10	-	-	-	-	-
[Tim] Gestor de Identidades	10	5%	-	-	-	-
[ERP] Infor LN	10	-	-	-	-	-
[BDD] Bases de Datos	10	-	-	-	-	-
[Sist_op] Sistemas Operativos	10	-	-	-	-	-
[pc] Equipos de usuarios	10	5%	-	-	-	-
[rack_srv] Racks de Servidores	10	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	10	-	-	-	-	-
[Sw] Switches	10	-	-	-	-	-
[Red_Lan] Red Lan	1	5%	-	-	-	-
[Red Wifi] Red Inalámbrica	1	5%	-	-	-	-

[firewall] Cortafuegos	1	5%	-	-	-	-
[Proy] Proyectores Digitales	10	5%	-	-	-	-
[Destruc] Destructoras de Papel	10	5%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	10	-	-	-	-	-

[E.25] Pérdida de equipos

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	5	1%	-	10%	-	-
[rack_srv] Racks de Servidores	1	100%	-	100%	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	100%	-	-
[Sw] Switches	1	-	-	100%	-	-
[Proy] Proyectores Digitales	1	10%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	0,1	-	-	100%	-	-

[A.3] Manipulación de los registros de actividad (log)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Backup] Respaldos	100	-	50%	-	-	-
[ERP] Infor LN	100	-	50%	-	-	-
[BDD] Bases de Datos	100	-	50%	-	-	-

[A.4] Manipulación de los ficheros de configuración

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[firewall] Cortafuegos	10	1%	10%	10%	-	-

[A.5] Suplantación de la identidad

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	0,2	-	100%	100%	100%	-
[Impresión] Impresoras Lexmark	0,2	-	100%	100%	100%	-
[Backup] Respaldos	0,2	-	100%	100%	100%	-
[Active Dir] Directorio Activo	1	-	50%	50%	100%	-
[Tim] Gestor de Identidades	1	-	50%	50%	100%	-
[ERP] Infor LN	0,2	-	100%	100%	100%	-
[BDD] Bases de Datos	0,2	-	100%	100%	100%	-
[Sist_op] Sistemas Operativos	0,2	-	100%	100%	100%	-
[pc] Equipos de usuarios	0,2	-	100%	100%	100%	-
[rack_srv] Racks de Servidores	0,2	-	100%	100%	100%	-
[Srv_intel] Servidores Intel Windows	0,2	-	100%	100%	100%	-
[Red_Lan] Red Lan	1	-	10%	50%	100%	-
[Red Wifi] Red Inalámbrica	1	-	10%	50%	100%	-
[firewall] Cortafuegos	1	-	10%	50%	100%	-
[fib] Fibra Óptica	1	-	10%	50%	100%	-
[Cuarto_srv] Cuarto de Servidores	0,2	-	100%	100%	100%	-

[A.6] Abuso de privilegios de acceso

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	10%	10%	100%	-
[Impresión] Impresoras Lexmark	10	-	10%	50%	-	-
[Backup] Respaldos	1	-	10%	10%	100%	-
[Active Dir] Directorio Activo	1	-	10%	10%	100%	-
[Tim] Gestor de Identidades	1	-	10%	10%	100%	-
[ERP] Infor LN	1	-	10%	10%	100%	-
[BDD] Bases de Datos	1	-	10%	10%	100%	-
[Sist_op] Sistemas Operativos	1	-	10%	10%	100%	-
[pc] Equipos de usuarios	1	-	10%	10%	100%	-
[rack_srv] Racks de Servidores	1	10%	100%	100%	-	-
[Srv_intel] Servidores Intel Windows	1	-	100%	100%	100%	-
[Red_Lan] Red Lan	1	-	10%	10%	100%	-
[Red Wifi] Red Inalámbrica	1	-	10%	10%	100%	-
[firewall] Cortafuegos	1	-	10%	10%	100%	-
[Proy] Proyectores Digitales	1	-	-	-	-	-
[Destruc] Destructoras de Papel	1	-	-	-	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	10%	10%	100%	-

[A.7] Uso no previsto

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	10%	10%	-	-
[Backup] Respaldos	1	-	10%	10%	-	-
[Active Dir] Directorio Activo	1	-	10%	10%	-	-
[Tim] Gestor de Identidades	1	-	10%	10%	-	-
[ERP] Infor LN	1	-	10%	10%	-	-
[BDD] Bases de Datos	1	-	10%	10%	-	-
[Sist_op] Sistemas Operativos	1	-	10%	10%	-	-
[pc] Equipos de usuarios	1	1%	1%	10%	-	-
[rack_srv] Racks de Servidores	1	10%	10%	100%	-	-
[Srv_intel] Servidores Intel Windows	1	-	10%	100%	-	-
[Sw] Switches	1	-	1%	10%	-	-
[Red_Lan] Red Lan	1	1%	10%	10%	-	-
[Red Wifi] Red Inalámbrica	1	1%	10%	10%	-	-
[firewall] Cortafuegos	1	1%	10%	10%	-	-
[Proy] Proyectores Digitales	1	5%	-	-	-	-
[Destruc] Destructoras de Papel	1	-	-	-	-	-
[Cub] Cubículos de Usuarios	1	5%	1%	1%	-	-
[fib] Fibra Óptica	1	-	1%	1%	-	-
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	1%	10%	-	-

[A.8] Difusión de software dañino

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	1	-	100%	100%	-	-
[BDD] Bases de Datos	1	-	100%	100%	-	-
[Sist_op] Sistemas	1	-	100%	100%	-	-

Operativos						

[A.9] [Re-]encaminamiento de mensajes

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	-	10%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	10%	-	-
[firewall] Cortafuegos	1	-	-	10%	-	-
[fib] Fibra Óptica	1	-	-	10%	-	-

[A.10] Alteración de secuencia

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	10%	-	-	-
[Red Wifi] Red Inalámbrica	1	-	10%	-	-	-
[firewall] Cortafuegos	1	-	10%	-	-	-
[fib] Fibra Óptica	1	-	10%	-	-	-

[A.11] Acceso no autorizado

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	10%	50%	100%	-
[Impresión] Impresoras Lexmark	100	-	10%	50%	-	-
[Backup] Respaldos	1	-	10%	50%	100%	-
[Active Dir] Directorio Activo	1	-	10%	50%	100%	-
[Tim] Gestor de Identidades	1	-	10%	50%	100%	-
[ERP] Infor LN	1	-	10%	50%	100%	-
[BDD] Bases de Datos	1	-	10%	50%	100%	-
[Sist_op] Sistemas Operativos	1	-	10%	50%	100%	-
[pc] Equipos de usuarios	1	1%	10%	50%	100%	-
[rack_srv] Racks de Servidores	1	10%	100%	100%	-	-
[Srv_intel] Servidores Intel Windows	1	-	100%	100%	100%	-
[Sw] Switches	1	-	10%	50%	-	-
[Red_Lan] Red Lan	1	-	10%	50%	100%	-
[Red Wifi] Red Inalámbrica	1	-	10%	50%	100%	-
[firewall] Cortafuegos	1	-	10%	50%	100%	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	10%	50%	100%	-

[A.12] Análisis de tráfico

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	-	2%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	2%	-	-
[firewall] Cortafuegos	1	-	-	2%	-	-
[fib] Fibra Óptica	1	-	-	2%	-	-

[A.13] Repudio (negación de actuaciones)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	-	-	100%
[Impresión] Impresoras Lexmark	1	-	-	-	-	100%

[Backup] Respaldos	1	-	-	-	-	100%
[Active Dir] Directorio Activo	5	-	-	-	-	100%
[Tim] Gestor de Identidades	5	-	-	-	-	100%
[ERP] Infor LN	1	-	-	-	-	100%
[BDD] Bases de Datos	1	-	-	-	-	100%
[Sist_op] Sistemas Operativos	1	-	-	-	-	100%
[pc] Equipos de usuarios	1	-	-	-	-	100%
[rack_srv] Racks de Servidores	1	-	-	-	-	100%
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	100%
[Red_Lan] Red Lan	1	-	-	-	-	100%
[Red Wifi] Red Inalámbrica	1	-	-	-	-	100%
[firewall] Cortafuegos	1	-	-	-	-	100%
[fib] Fibra Óptica	1	-	-	-	-	100%
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	100%

[A.14] Interceptación de información (escucha)

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Red_Lan] Red Lan	1	-	-	1%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	5%	-	-
[firewall] Cortafuegos	1	-	-	10%	-	-
[fib] Fibra Óptica	1	-	-	5%	-	-

[A.15] Modificación de la información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	50%	-	-	-
[Impresión] Impresoras Lexmark	1	-	50%	-	-	-
[Backup] Respaldos	1	-	50%	-	-	-
[Active Dir] Directorio Activo	10	-	50%	-	-	-
[Tim] Gestor de Identidades	10	-	50%	-	-	-
[ERP] Infor LN	1	-	50%	-	-	-
[BDD] Bases de Datos	1	-	50%	-	-	-
[Sist_op] Sistemas Operativos	1	-	50%	-	-	-
[pc] Equipos de usuarios	1	-	50%	-	-	-
[rack_srv] Racks de Servidores	1	-	50%	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	50%	-	-	-
[Red_Lan] Red Lan	1	-	10%	-	-	-
[Red Wifi] Red Inalámbrica	1	-	10%	-	-	-
[firewall] Cortafuegos	1	-	10%	-	-	-
[fib] Fibra Óptica	1	-	10%	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	50%	-	-	-

[A.18] Destrucción de la información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	-	-	-
[Impresión] Impresoras Lexmark	1	5%	-	-	-	-
[Backup] Respaldos	1	-	-	-	-	-

[Active Dir] Directorio Activo	1	-	-	-	-	-
[Tim] Gestor de Identidades	1	5%	-	-	-	-
[ERP] Infor LN	1	-	-	-	-	-
[BDD] Bases de Datos	1	-	-	-	-	-
[Sist_op] Sistemas Operativos	1	-	-	-	-	-
[pc] Equipos de usuarios	1	5%	-	-	-	-
[rack_srv] Racks de Servidores	1	50%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Red_Lan] Red Lan	1	5%	-	-	-	-
[Red Wifi] Red Inalámbrica	1	5%	-	-	-	-
[firewall] Cortafuegos	1	5%	-	-	-	-
[Proy] Proyectores Digitales	1	5%	-	-	-	-
[Destruc] Destructoras de Papel	1	5%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

[A.19] Revelación de información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	50%	-	-
[Impresión] Impresoras Lexmark	1	-	-	50%	-	-
[Backup] Respaldos	1	-	-	50%	-	-
[ERP] Infor LN	1	-	-	50%	-	-
[BDD] Bases de Datos	1	-	-	50%	-	-
[Sist_op] Sistemas Operativos	1	-	-	50%	-	-
[pc] Equipos de usuarios	1	-	-	50%	-	-
[rack_srv] Racks de Servidores	1	-	-	50%	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	50%	-	-
[Red_Lan] Red Lan	1	-	-	50%	-	-
[Red Wifi] Red Inalámbrica	1	-	-	50%	-	-
[firewall] Cortafuegos	1	-	-	50%	-	-
[fib] Fibra Óptica	1	-	-	50%	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	50%	-	-

[A.22] Manipulación de programas

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[ERP] Infor LN	1	-	100%	100%	-	-
[BDD] Bases de Datos	1	-	100%	100%	-	-
[Sist_op] Sistemas Operativos	1	-	100%	100%	-	-

[A.23] Manipulación del hardware

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	0,5	5%	-	50%	-	-
[Sw] Switches	0,5	-	-	50%	-	-
[Proy] Proyectores Digitales	1	5%	-	-	-	-
[Destruc] Destructoras de Papel	1	-	-	-	-	-
[Cub] Cubículos de Usuarios	1	5%	-	50%	-	-
[fib] Fibra Óptica	1	-	-	50%	-	-
[Cuarto_srv] Cuarto de	0,5	-	-	50%	-	-

Servidores						

[A.24] Denegación de servicio

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	1	-	-	-	-	-
[Impresión] Impresoras Lexmark	1	5%	-	-	-	-
[Backup] Respaldos	1	-	-	-	-	-
[Active Dir] Directorio Activo	10	-	-	-	-	-
[Tim] Gestor de Identidades	10	5%	-	-	-	-
[ERP] Infor LN	1	-	-	-	-	-
[BDD] Bases de Datos	1	-	-	-	-	-
[Sist_op] Sistemas Operativos	1	-	-	-	-	-
[pc] Equipos de usuarios	2	10%	-	-	-	-
[rack_srv] Racks de Servidores	2	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	2	-	-	-	-	-
[Sw] Switches	2	-	-	-	-	-
[Red_Lan] Red Lan	10	5%	-	-	-	-
[Red Wifi] Red Inalámbrica	10	5%	-	-	-	-
[firewall] Cortafuegos	10	5%	-	-	-	-
[Proy] Proyectores Digitales	2	10%	-	-	-	-
[Destruc] Destructoras de Papel	10	5%	-	-	-	-
[fib] Fibra Óptica	10	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	2	-	-	-	-	-

[A.25] Robo de equipos

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	5	1%	-	10%	-	-
[rack_srv] Racks de Servidores	0,1	100%	-	100%	-	-
[Srv_intel] Servidores Intel Windows	0,1	-	-	100%	-	-
[Sw] Switches	0,1	-	-	100%	-	-
[Proy] Proyectores Digitales	0,5	1%	-	-	-	-
[Cub] Cubículos de Usuarios	0,5	1%	-	50%	-	-
[fib] Fibra Óptica	0,8	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	0,1	-	-	100%	-	-

[A.26] Ataque destructivo

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[pc] Equipos de usuarios	1	10%	-	-	-	-
[rack_srv] Racks de Servidores	1	100%	-	-	-	-
[Srv_intel] Servidores Intel Windows	1	-	-	-	-	-
[Sw] Switches	1	-	-	-	-	-
[Proy] Proyectores Digitales	1	1%	-	-	-	-
[Cub] Cubículos de Usuarios	1	1%	-	-	-	-
[fib] Fibra Óptica	1	-	-	-	-	-
[edificio] Inverna	0,1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	0,1	-	-	-	-	-

[A.27] Ocupación enemiga

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	1	-	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	1	-	-	-	-	-

Según (Amutio, 2012), cuando un activo es víctima de una amenaza, no se afecta en el mismo valor, cabe indicar que, si las amenazas perjudican a los activos, se debe valorar su influencia en el valor del activo:

- Degradación: "Cuán perjudicado resultaría el valor del activo".
- Probabilidad: "Cuán probable o improbable es que se materialice la amenaza".

(Amutio, 2012), menciona que es usual utilizar un (1) año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra.

La tabla 17 muestra como calificará la probabilidad de que se materialicen amenazas en base a la metodología MAGERIT:

Tabla 17
Tabla de probabilidad de ocurrencia

MA	1OO	Muy frecuente	A diario
A	10	Frecuente	Mensual
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

3.11 Análisis de impacto acumulado

El impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza. Al conocer el valor de los activos (en sus distintas dimensiones) y la degradación que causan las amenazas, se pude identificar el impacto que estas causarían sobre el sistema.

El impacto se calcula para cada activo de información, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

Las fases que se han contemplado para el proyecto son los siguientes:

- [potencial]
- [current] situación actual
- [target] situación objetivo
- [PILAR] recomendación

Con la ayuda de la herramienta PILAR, se han obtenido los siguientes resultados:

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[10]	[10]	[10]	[10]	[10]
[Email] Mensajería	[9]	[9]	[9]	[7]	[6]
[Impresión] Impresoras	[1]	[1]	[1]	[1]	[1]
[Backup] Respaldos	[10]	[10]	[10]	[9]	[10]
[Active Dir] Directorio Activo	[8]	[6]	[8]	[8]	[7]
[Tim] Gestor de Identidades	[4]	[5]	[7]	[7]	[7]
[ERP] Infor LN	[10]	[10]	[10]	[10]	[10]
[BDD] Bases de Datos	[10]	[10]	[10]	[10]	[10]
[Sist_op] Sistemas Operativos	[8]	[7]	[7]	[7]	[7]
[pc] Equipos de usuarios	[6]	[7]	[7]	[9]	[8]
[rack_srv] Racks de Servidores	[2]	[1]	[0]	[1]	[0]
[Srv_intel] Servidores Intel Windows	[8]	[8]	[7]	[8]	[7]
[Sw] Switches	[9]	[0]	[0]	[3]	[2]
[Red_Lan] Red Lan	[7]	[4]	[4]	[3]	[6]
[Red Wifi] Red Inalàmbrica	[7]	[4]	[4]	[3]	[6]
[firewall] Cortafuegos	[9]	[4]	[3]	[6]	[4]
[Proy] Proyectores Digitales	[2]				
[Destruc] Destructoras de Papel	[0]				
[Cub] Cubículos de Usuarios	[0]	[4]	[6]	[6]	[6]
[fib] Fibra Óptica	[7]	[1]	[2]	[1]	[1]
[edificio] Inverna	[9]	[7]	[6]	[7]	[8]
[Cuarto_srv] Cuarto de Servidores	[9]	[8]	[8]	[8]	[9]

Figura 24 Valoración de impacto acumulado

A continuación, se muestra el detalle de las valoraciones de impacto acumulado por cada activo:

- Fase: [potencial]

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	[0]	[10]	[10]	[10]	[10]
[Impresión] Impresoras	[6]	[10]	[10]	[10]	[10]
[Backup] Respaldos	[0]	[10]	[10]	[10]	[10]
[Active Dir] Directorio Activo	[0]	[9]	[9]	[10]	[10]
[Tim] Gestor de Identidades	[6]	[9]	[9]	[10]	[10]

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	[0]	[10]	[10]	[10]	[10]
[ERP] Infor LN	[0]	[10]	[10]	[10]	[10]
[BDD] Bases de Datos	[0]	[10]	[10]	[10]	[10]
[Sist_op] Sistemas Operativos	[0]	[10]	[10]	[10]	[10]
[HW] Equipos	[10]	[10]	[10]	[10]	[10]
[pc] Equipos de usuarios	[7]	[10]	[10]	[10]	[10]
[rack_srv] Racks de Servidores	[10]	[10]	[10]	[10]	[10]
[Srv] Servidores de Centro de Datos	[0]	[10]	[10]	[10]	[10]
[Srv_intel] Servidores Intel Windows	[0]	[10]	[10]	[10]	[10]
[Sw] Switches	[0]	[7]	[10]		
[COM] Comunicaciones	[6]	[8]	[9]	[10]	[10]
[Red_Lan] Red Lan	[6]	[8]	[9]	[10]	[10]
[Red Wifi] Red Inalámbrica	[6]	[8]	[9]	[10]	[10]
[firewall] Cortafuegos	[6]	[8]	[9]	[10]	[10]
[AUX] Elementos auxiliares	[7]	[8]	[9]	[10]	[10]
[Proy] Proyectores Digitales	[7]				
[Destruc] Destructoras de Papel	[6]				
[Cub] Cubículos de Usuarios	[7]	[4]	[9]		
[fib] Fibra Óptica	[0]	[8]	[9]	[10]	[10]

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	[0]				
[Cuarto_srv] Cuarto de Servidores	[0]	[10]	[10]	[10]	[10]

- Fase: [current] situación actual

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	[0]	[8]	[8]	[8]	[8]
[Impresión] Impresoras	[5]	[8]	[9]	[8]	[9]
[Backup] Respaldos	[0]	[8]	[9]	[8]	[9]
[Active Dir] Directorio Activo	[0]	[7]	[8]	[8]	[9]
[Tim] Gestor de Identidades	[4]	[7]	[8]	[8]	[9]

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	[0]	[9]	[9]	[9]	[9]
[ERP] Infor LN	[0]	[9]	[9]	[9]	[9]
[BDD] Bases de Datos	[0]	[9]	[9]	[9]	[9]
[Sist_op] Sistemas Operativos	[0]	[9]	[9]	[9]	[9]
[HW] Equipos	[9]	[8]	[9]	[8]	[9]
[pc] Equipos de usuarios	[6]	[8]	[9]	[8]	[9]
[rack_srv] Racks de Servidores	[9]	[8]	[8]	[8]	[8]
[Srv] Servidores de Centro de Datos	[0]	[8]	[8]	[8]	[9]
[Srv_intel] Servidores Intel Windows	[0]	[8]	[8]	[8]	[9]
[Sw] Switches	[0]	[5]	[8]		
[COM] Comunicaciones	[4]	[6]	[7]	[8]	[8]
[Red_Lan] Red Lan	[4]	[6]	[7]	[8]	[8]
[Red Wifi] Red Inalámbrica	[4]	[6]	[7]	[8]	[8]
[firewall] Cortafuegos	[4]	[6]	[7]	[8]	[8]
[AUX] Elementos auxiliares	[6]	[6]	[7]	[8]	[8]
[Proy] Proyectores Digitales	[6]				
[Destruc] Destructoras de Papel	[4]				
[Cub] Cubículos de Usuarios	[5]	[2]	[7]		
[fib] Fibra Óptica	[0]	[6]	[7]	[8]	[8]

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	[0]				
[Cuarto_srv] Cuarto de Servidores	[0]	[8]	[9]	[8]	[9]

- Fase: [target] situación objetivo

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	[0]	[7]	[7]	[7]	[6]
[Impresión] Impresoras	[3]	[7]	[7]	[7]	[7]
[Backup] Respaldos	[0]	[7]	[7]	[7]	[7]
[Active Dir] Directorio Activo	[0]	[6]	[6]	[7]	[7]
[Tim] Gestor de Identidades	[2]	[6]	[6]	[7]	[7]

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	[0]	[7]	[7]	[7]	[7]
[ERP] Infor LN	[0]	[7]	[7]	[7]	[7]
[BDD] Bases de Datos	[0]	[7]	[7]	[7]	[6]
[Sist_op] Sistemas Operativos	[0]	[7]	[7]	[7]	[6]
[HW] Equipos	[7]	[7]	[7]	[7]	[7]
[pc] Equipos de usuarios	[4]	[7]	[7]	[7]	[7]
[rack_srv] Racks de Servidores	[7]	[7]	[7]	[7]	[7]
[Srv] Servidores de Centro de Datos	[0]	[7]	[7]	[7]	[6]
[Srv_intel] Servidores Intel	[0]	[7]	[7]	[7]	[6]

Windows					
[Sw] Switches	[0]	[3]	[6]		
[COM] Comunicaciones	[3]	[5]	[6]	[7]	[6]
[Red_Lan] Red Lan	[2]	[5]	[6]	[7]	[6]
[Red Wifi] Red Inalámbrica	[2]	[5]	[6]	[7]	[6]
[firewall] Cortafuegos	[3]	[5]	[6]	[7]	[6]
[AUX] Elementos auxiliares	[4]	[5]	[6]	[6]	[6]
[Proy] Proyectores Digitales	[4]				
[Destruc] Destructoras de Papel	[2]				
[Cub] Cubículos de Usuarios	[3]	[0]	[5]		
[fib] Fibra Óptica	[0]	[5]	[6]	[6]	[6]

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	[0]				
[Cuarto_srv] Cuarto de Servidores	[0]	[7]	[7]	[7]	[7]

- Fase: [PILAR] recomendación

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	[0]	[6]	[6]	[6]	[6]
[Impresión] Impresoras	[2]	[6]	[5]	[6]	[6]
[Backup] Respaldos	[0]	[6]	[6]	[6]	[6]
[Active Dir] Directorio Activo	[0]	[5]	[5]	[6]	[6]
[Tim] Gestor de Identidades	[2]	[5]	[5]	[6]	[6]

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	[0]	[6]	[6]	[6]	[6]
[ERP] Infor LN	[0]	[6]	[6]	[6]	[6]
[BDD] Bases de Datos	[0]	[6]	[6]	[6]	[6]
[Sist_op] Sistemas Operativos	[0]	[6]	[6]	[6]	[6]
[HW] Equipos	[6]	[6]	[6]	[6]	[6]
[pc] Equipos de usuarios	[3]	[6]	[5]	[6]	[6]
[rack_srv] Racks de Servidores	[6]	[6]	[6]	[6]	[6]
[Srv] Servidores de Centro de Datos	[0]	[6]	[6]	[6]	[6]
[Srv_intel] Servidores Intel Windows	[0]	[6]	[6]	[6]	[6]
[Sw] Switches	[0]	[3]	[6]		
[COM] Comunicaciones	[2]	[4]	[5]	[6]	[6]
[Red_Lan] Red Lan	[2]	[4]	[5]	[6]	[6]
[Red Wifi] Red Inalámbrica	[2]	[4]	[5]	[6]	[6]
[firewall] Cortafuegos	[2]	[4]	[5]	[6]	[6]
[AUX] Elementos auxiliares	[3]	[4]	[5]	[6]	[6]
[Proy] Proyectores Digitales	[3]				
[Destruc] Destructoras de Papel	[2]				
[Cub] Cubículos de Usuarios	[3]	[0]	[5]		
[fib] Fibra Óptica	[0]	[4]	[5]	[6]	[6]

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	[0]				
[Cuarto_srv] Cuarto de Servidores	[0]	[6]	[6]	[6]	[6]

A nivel de los parámetros de seguridad, las calificaciones de los activos se han distribuido en cuatro fases: potencial, actual, objetivo, PILAR:

- [D] disponibilidad

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	[0]	[0]	[0]	[0]
[Impresión] Impresoras	[6]	[5]	[3]	[2]
[Backup] Respaldos	[0]	[0]	[0]	[0]
[Active Dir] Directorio Activo	[0]	[0]	[0]	[0]
[Tim] Gestor de Identidades	[6]	[4]	[2]	[2]

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	[0]	[0]	[0]	[0]
[ERP] Infor LN	[0]	[0]	[0]	[0]
[BDD] Bases de Datos	[0]	[0]	[0]	[0]
[Sist_op] Sistemas Operativos	[0]	[0]	[0]	[0]
[HW] Equipos	[10]	[9]	[7]	[6]
[pc] Equipos de usuarios	[7]	[6]	[4]	[3]
[rack_srv] Racks de Servidores	[10]	[9]	[7]	[6]
[Srv] Servidores de Centro de Datos	[0]	[0]	[0]	[0]
[Srv_intel] Servidores Intel Windows	[0]	[0]	[0]	[0]
[Sw] Switches	[0]	[0]	[0]	[0]
[COM] Comunicaciones	[6]	[4]	[3]	[2]
[Red_Lan] Red Lan	[6]	[4]	[2]	[2]
[Red Wifi] Red Inalámbrica	[6]	[4]	[2]	[2]
[firewall] Cortafuegos	[6]	[4]	[3]	[2]
[AUX] Elementos auxiliares	[7]	[6]	[4]	[3]
[Proy] Proyectores Digitales	[7]	[6]	[4]	[3]
[Destruc] Destructoras de Papel	[6]	[4]	[2]	[2]
[Cub] Cubículos de Usuarios	[7]	[5]	[3]	[3]
[fib] Fibra Óptica	[0]	[0]	[0]	[0]

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	[0]	[0]	[0]	[0]
[Cuarto_srv] Cuarto de Servidores	[0]	[0]	[0]	[0]

- [I] integridad de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	[10]	[8]	[7]	[6]
[Impresión] Impresoras	[10]	[8]	[7]	[6]
[Backup] Respaldos	[10]	[8]	[7]	[6]
[Active Dir] Directorio Activo	[9]	[7]	[6]	[5]
[Tim] Gestor de Identidades	[9]	[7]	[6]	[5]

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	[10]	[9]	[7]	[6]
[ERP] Infor LN	[10]	[9]	[7]	[6]
[BDD] Bases de Datos	[10]	[9]	[7]	[6]
[Sist_op] Sistemas Operativos	[10]	[9]	[7]	[6]
[HW] Equipos	[10]	[8]	[7]	[6]
[pc] Equipos de usuarios	[10]	[8]	[7]	[6]
[rack_srv] Racks de Servidores	[10]	[8]	[7]	[6]
[Srv] Servidores de Centro de Datos	[10]	[8]	[7]	[6]
[Srv_intel] Servidores Intel Windows	[10]	[8]	[7]	[6]
[Sw] Switches	[7]	[5]	[3]	[3]
[COM] Comunicaciones	[8]	[6]	[5]	[4]
[Red_Lan] Red Lan	[8]	[6]	[5]	[4]
[Red Wifi] Red Inalámbrica	[8]	[6]	[5]	[4]
[firewall] Cortafuegos	[8]	[6]	[5]	[4]
[AUX] Elementos auxiliares	[8]	[6]	[5]	[4]
[Proy] Proyectores Digitales				
[Destruc] Destructoras de Papel				
[Cub] Cubículos de Usuarios	[4]	[2]	[0]	[0]
[fib] Fibra Óptica	[8]	[6]	[5]	[4]

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna				
[Cuarto_srv] Cuarto de Servidores	[10]	[8]	[7]	[6]

- [C] confidencialidad de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	[10]	[8]	[7]	[6]
[Impresión] Impresoras	[10]	[9]	[7]	[5]
[Backup] Respaldos	[10]	[9]	[7]	[6]
[Active Dir] Directorio Activo	[9]	[8]	[6]	[5]
[Tim] Gestor de Identidades	[9]	[8]	[6]	[5]

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	[10]	[9]	[7]	[6]
[ERP] Infor LN	[10]	[9]	[7]	[6]
[BDD] Bases de Datos	[10]	[9]	[7]	[6]
[Sist_op] Sistemas Operativos	[10]	[9]	[7]	[6]
[HW] Equipos	[10]	[9]	[7]	[6]
[pc] Equipos de usuarios	[10]	[9]	[7]	[5]
[rack_srv] Racks de Servidores	[10]	[8]	[7]	[6]
[Srv] Servidores de Centro de Datos	[10]	[8]	[7]	[6]
[Srv_intel] Servidores Intel Windows	[10]	[8]	[7]	[6]
[Sw] Switches	[10]	[8]	[6]	[6]
[COM] Comunicaciones	[9]	[7]	[6]	[5]
[Red_Lan] Red Lan	[9]	[7]	[6]	[5]
[Red Wifi] Red Inalámbrica	[9]	[7]	[6]	[5]
[firewall] Cortafuegos	[9]	[7]	[6]	[5]
[AUX] Elementos auxiliares	[9]	[7]	[6]	[5]
[Proy] Proyectores Digitales				
[Destruc] Destructoras de Papel				
[Cub] Cubículos de Usuarios	[9]	[7]	[5]	[5]
[fib] Fibra Óptica	[9]	[7]	[6]	[5]

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna				
[Cuarto_srv] Cuarto de Servidores	[10]	[9]	[7]	[6]

- [A] autenticidad de los usuarios y de la información

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	[10]	[8]	[7]	[6]
[Impresión] Impresoras	[10]	[8]	[7]	[6]
[Backup] Respaldos	[10]	[8]	[7]	[6]
[Active Dir] Directorio Activo	[10]	[8]	[7]	[6]
[Tim] Gestor de Identidades	[10]	[8]	[7]	[6]

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	[10]	[9]	[7]	[6]
[ERP] Infor LN	[10]	[9]	[7]	[6]
[BDD] Bases de Datos	[10]	[9]	[7]	[6]
[Sist_op] Sistemas Operativos	[10]	[9]	[7]	[6]
[HW] Equipos	[10]	[8]	[7]	[6]
[pc] Equipos de usuarios	[10]	[8]	[7]	[6]
[rack_srv] Racks de Servidores	[10]	[8]	[7]	[6]
[Srv] Servidores de Centro de Datos	[10]	[8]	[7]	[6]
[Srv_intel] Servidores Intel Windows	[10]	[8]	[7]	[6]
[Sw] Switches				

[COM] Comunicaciones	[10]	[8]	[7]	[6]
[Red_Lan] Red Lan	[10]	[8]	[7]	[6]
[Red Wifi] Red Inalámbrica	[10]	[8]	[7]	[6]
[firewall] Cortafuegos	[10]	[8]	[7]	[6]
[AUX] Elementos auxiliares	[10]	[8]	[6]	[6]
[Proy] Proyectores Digitales				
[Destruc] Destructoras de Papel				
[Cub] Cubículos de Usuarios				
[fib] Fibra Óptica	[10]	[8]	[6]	[6]

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna				
[Cuarto_srv] Cuarto de Servidores	[10]	[8]	[7]	[6]

- [T] trazabilidad del servicio y de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	[10]	[8]	[6]	[6]
[Impresión] Impresoras	[10]	[9]	[7]	[6]
[Backup] Respaldos	[10]	[9]	[7]	[6]
[Active Dir] Directorio Activo	[10]	[9]	[7]	[6]
[Tim] Gestor de Identidades	[10]	[9]	[7]	[6]

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	[10]	[9]	[7]	[6]
[ERP] Infor LN	[10]	[9]	[7]	[6]
[BDD] Bases de Datos	[10]	[9]	[6]	[6]
[Sist_op] Sistemas Operativos	[10]	[9]	[6]	[6]
[HW] Equipos	[10]	[9]	[7]	[6]
[pc] Equipos de usuarios	[10]	[9]	[7]	[6]
[rack_srv] Racks de Servidores	[10]	[8]	[7]	[6]
[Srv] Servidores de Centro de Datos	[10]	[9]	[6]	[6]
[Srv_intel] Servidores Intel Windows	[10]	[9]	[6]	[6]
[Sw] Switches				
[COM] Comunicaciones	[10]	[8]	[6]	[6]
[Red_Lan] Red Lan	[10]	[8]	[6]	[6]
[Red Wifi] Red Inalámbrica	[10]	[8]	[6]	[6]
[firewall] Cortafuegos	[10]	[8]	[6]	[6]
[AUX] Elementos auxiliares	[10]	[8]	[6]	[6]
[Proy] Proyectores Digitales				
[Destruc] Destructoras de Papel				
[Cub] Cubículos de Usuarios				
[fib] Fibra Óptica	[10]	[8]	[6]	[6]

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna				
[Cuarto_srv] Cuarto de Servidores	[10]	[9]	[7]	[6]

3.12 Análisis de riesgo acumulado

Para este análisis se realiza un cálculo sobre un activo de información considerando el impacto acumulado sobre un activo debido a una amenaza. Los niveles de criticidad para calificar los riesgos se muestran en la tabla 18; en base a la herramienta PILAR y acorde a la metodología MAGERIT:

Tabla 18
Niveles de criticidad de riesgo

{0}	Despreciable
{1}	Bajo
{2}	Medio
{3}	Alto
{4}	Muy alto
{5}	Crítico
{6}	Muy crítico
{7}	Extremadamente crítico
{8}	Desastre
{9}	Catástrofe

Con la ayuda de la herramienta PILAR, se ha obtenido los riesgos que afectan a los cinco parámetros de seguridad:

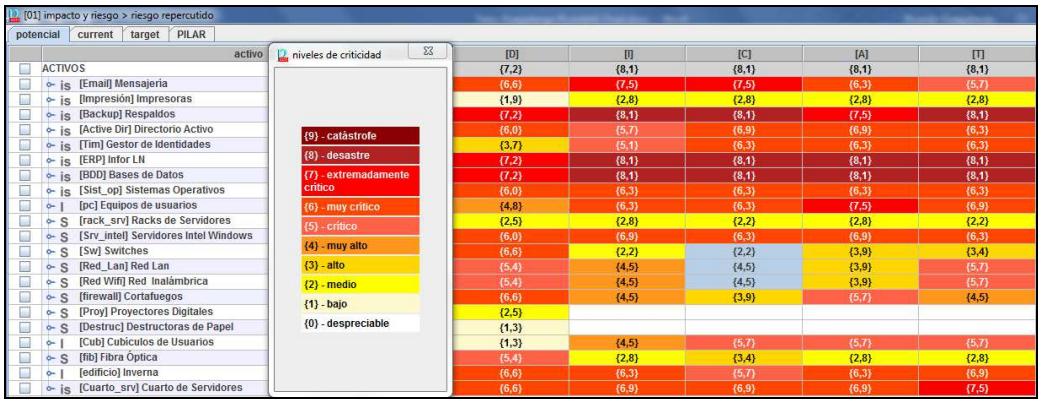


Figura 25 Valoración de riesgo acumulado

Estableciendo una media de las valoraciones emitidas; la figura 26, identifica los activos de información con mayor nivel de riesgo:

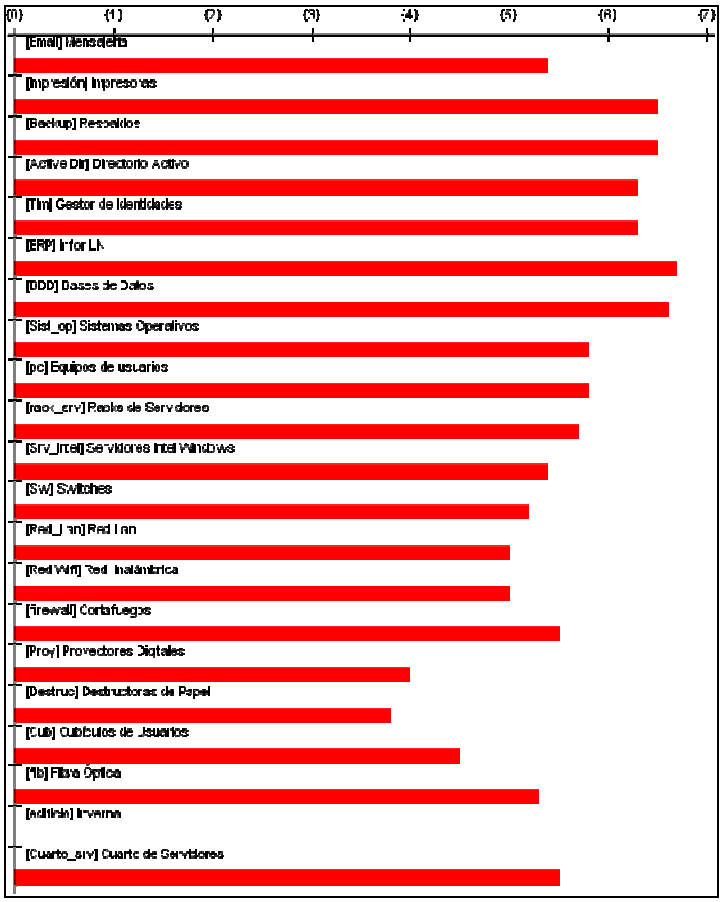


Figura 26 Nivel de riesgo por activo

Se identifica que los activos que presentan mayores riesgos son:

- ERP Infor LN
- Bases de datos

A continuación, se muestra el detalle de las valoraciones de riesgo acumulado por cada activo y fase:

- Fase: [potencial]

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	{0}	{6,3}	{6,3}	{6,8}	{6,8}
[Impresión] Impresoras	{4,5}	{6,8}	{8,1}	{6,2}	{6,8}
[Backup] Respaldos	{0}	{8,1}	{6,3}	{6,8}	{6,8}
[Active Dir] Directorio Activo	{0}	{7,2}	{6,3}	{6,8}	{7,4}
[Tim] Gestor de Identidades	{5,4}	{7,2}	{6,3}	{6,8}	{7,4}

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	{0}	{8,1}	{6,8}	{6,8}	{6,8}
[ERP] Infor LN	{0}	{8,1}	{6,8}	{6,8}	{6,8}
[BDD] Bases de Datos	{0}	{8,1}	{6,8}	{6,8}	{6,8}
[Sist_op] Sistemas Operativos	{0}	{6,8}	{6,8}	{6,8}	{6,8}
[HW] Equipos	{7,2}	{6,8}	{6,8}	{6,8}	{6,8}
[pc] Equipos de usuarios	{5,4}	{6,3}	{6,3}	{6,8}	{6,8}
[rack_srv] Racks de Servidores	{7,2}	{6,8}	{6,8}	{6,2}	{6,8}
[Srv] Servidores de Centro de Datos	{0}	{6,8}	{6,8}	{6,8}	{6,8}
[Srv_intel] Servidores Intel Windows	{0}	{6,8}	{6,8}	{6,8}	{6,8}
[Sw] Switches	{0}	{5,1}	{6,8}	-	-
[COM] Comunicaciones	{5,4}	{5,9}	{6,3}	{6,8}	{6,8}
[Red_Lan] Red Lan	{5,4}	{5,6}	{6,3}	{6,8}	{6,8}
[Red Wifi] Red Inalámbrica	{5,4}	{5,6}	{6,3}	{6,8}	{6,8}
[firewall] Cortafuegos	{5,4}	{5,9}	{6,3}	{6,8}	{6,8}
[AUX] Elementos auxiliares	{5,4}	{5,6}	{6,3}	{6,8}	{6,8}
[Proy] Proyectores Digitales	{5,4}	-	-	-	-
[Destruc] Destructoras de Papel	{5,4}	-	-	-	-
[Cub] Cubículos de Usuarios	{4,8}	{3,3}	{6,3}	-	-
[fib] Fibra Óptica	{0}	{5,6}	{6,3}	{6,8}	{6,8}

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	{0}	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{0}	{6,3}	{6,3}	{6,8}	{6,8}

- Fase: [current] situación actual

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	{0}	{4,5}	{4,7}	{5,0}	{5,4}
[Impresión] Impresoras	{3,2}	{5,2}	{6,6}	{4,7}	{5,7}
[Backup] Respaldos	{0}	{6,5}	{4,8}	{5,2}	{5,7}
[Active Dir] Directorio Activo	{0}	{5,5}	{5,0}	{5,3}	{6,3}
[Tim] Gestor de Identidades	{3,9}	{5,5}	{5,0}	{5,3}	{6,3}

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	{0}	{6,8}	{5,9}	{5,5}	{6,0}
[ERP] Infor LN	{0}	{6,8}	{5,9}	{5,5}	{6,0}
[BDD] Bases de Datos	{0}	{6,6}	{5,7}	{5,2}	{5,8}
[Sist_op] Sistemas Operativos	{0}	{5,7}	{5,8}	{5,2}	{5,8}
[HW] Equipos	{5,7}	{5,3}	{5,4}	{5,2}	{5,8}
[pc] Equipos de usuarios	{4,1}	{4,7}	{4,9}	{5,2}	{5,8}
[rack_srv] Racks de Servidores	{5,7}	{5,3}	{5,3}	{4,6}	{5,3}
[Srv] Servidores de Centro de Datos	{0}	{5,1}	{5,4}	{5,1}	{5,4}
[Srv_intel] Servidores Intel Windows	{0}	{5,1}	{5,4}	{5,1}	{5,4}
[Sw] Switches	{0}	{3,5}	{5,2}	-	-
[COM] Comunicaciones	{3,6}	{4,2}	{4,7}	{5,1}	{5,5}
[Red_Lan] Red Lan	{3,3}	{3,7}	{4,4}	{4,9}	{5,0}
[Red Wifi] Red Inalámbrica	{3,4}	{3,7}	{4,4}	{4,9}	{5,0}
[firewall] Cortafuegos	{3,6}	{4,2}	{4,7}	{5,1}	{5,5}
[AUX] Elementos auxiliares	{4,0}	{3,9}	{4,6}	{5,0}	{5,3}
[Proy] Proyectores Digitales	{4,0}	-	-	-	-
[Destruc] Destructoras de Papel	{3,8}	-	-	-	-
[Cub] Cubículos de Usuarios	{3,3}	{1,5}	{4,5}	-	-
[fib] Fibra Óptica	{0}	{3,9}	{4,6}	{5,0}	{5,3}

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	{0}	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{0}	{4,6}	{4,7}	{5,1}	{5,5}

- Fase: [target] situación objetivo

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	{0}	{3,7}	{3,4}	{4,2}	{3,7}
[Impresión] Impresoras	{1,6}	{4,5}	{5,5}	{3,8}	{4,0}
[Backup] Respaldos	{0}	{5,4}	{3,4}	{4,3}	{3,8}
[Active Dir] Directorio Activo	{0}	{4,7}	{3,5}	{4,3}	{4,5}
[Tim] Gestor de Identidades	{2,2}	{4,7}	{3,5}	{4,3}	{4,5}

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	{0}	{5,4}	{3,6}	{4,2}	{3,9}
[ERP] Infor LN	{0}	{5,4}	{3,6}	{4,2}	{3,9}
[BDD] Bases de Datos	{0}	{5,3}	{3,3}	{4,2}	{3,7}
[Sist_op] Sistemas Operativos	{0}	{3,6}	{3,4}	{4,2}	{3,7}
[HW] Equipos	{4,2}	{4,2}	{4,2}	{4,3}	{3,9}
[pc] Equipos de usuarios	{2,4}	{3,7}	{3,5}	{4,3}	{3,9}
[rack_srv] Racks de Servidores	{4,2}	{3,8}	{3,8}	{3,2}	{3,8}
[Srv] Servidores de Centro de Datos	{0}	{4,2}	{4,2}	{4,2}	{3,7}
[Srv_intel] Servidores Intel Windows	{0}	{4,2}	{4,2}	{4,2}	{3,7}
[Sw] Switches	{0}	{1,8}	{3,6}	-	-
[COM] Comunicaciones	{2,2}	{3,1}	{3,4}	{4,0}	{3,6}
[Red_Lan] Red Lan	{2,0}	{2,7}	{3,4}	{3,9}	{3,4}
[Red Wifi] Red Inalámbrica	{2,0}	{2,6}	{3,4}	{3,9}	{3,4}
[firewall] Cortafuegos	{2,2}	{3,1}	{3,3}	{4,0}	{3,6}
[AUX] Elementos auxiliares	{2,3}	{2,7}	{3,4}	{3,7}	{3,6}
[Proy] Proyectores Digitales	{2,3}	-	-	-	-
[Destruc] Destructoras de Papel	{2,1}	-	-	-	-
[Cub] Cubículos de Usuarios	{1,6}	{0,76}	{2,8}	-	-
[fib] Fibra Óptica	{0}	{2,7}	{3,4}	{3,7}	{3,6}

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	{0}	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{0}	{3,5}	{3,4}	{4,2}	{3,8}

- Fase: [PILAR] recomendación

[IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]
[Email] Mensajería	{0}	{2,5}	{2,5}	{3,2}	{3,3}
[Impresión] Impresoras	{0,99}	{3,0}	{4,2}	{2,3}	{3,3}
[Backup] Respaldos	{0}	{4,3}	{2,5}	{3,2}	{3,4}
[Active Dir] Directorio Activo	{0}	{3,4}	{2,5}	{3,2}	{4,0}
[Tim] Gestor de Identidades	{1,8}	{3,4}	{2,5}	{3,2}	{4,0}

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW] Aplicaciones	{0}	{4,3}	{3,1}	{3,3}	{3,3}
[ERP] Infor LN	{0}	{4,3}	{3,1}	{3,3}	{3,3}
[BDD] Bases de Datos	{0}	{4,3}	{3,1}	{3,3}	{3,3}
[Sist_op] Sistemas Operativos	{0}	{3,2}	{3,1}	{3,3}	{3,3}
[HW] Equipos	{3,6}	{3,3}	{3,3}	{3,2}	{3,3}
[pc] Equipos de usuarios	{1,8}	{2,4}	{2,4}	{3,2}	{3,3}
[rack_srv] Racks de Servidores	{3,6}	{3,3}	{3,3}	{2,7}	{3,3}
[Srv] Servidores de Centro de Datos	{0}	{3,2}	{3,3}	{3,2}	{3,3}
[Srv_intel] Servidores Intel Windows	{0}	{3,2}	{3,3}	{3,2}	{3,3}
[Sw] Switches	{0}	{1,5}	{3,3}	-	-

[COM] Comunicaciones	{1,9}	{2,2}	{2,5}	{3,3}	{3,2}
[Red_Lan] Red Lan	{1,8}	{1,8}	{2,5}	{3,2}	{3,2}
[Red Wifi] Red Inalámbrica	{1,9}	{1,8}	{2,5}	{3,2}	{3,2}
[firewall] Cortafuegos	{1,8}	{2,2}	{2,5}	{3,3}	{3,2}
[AUX] Elementos auxiliares	{1,9}	{1,9}	{2,8}	{3,3}	{3,1}
[Proy] Proyectores Digitales	{1,9}	-	-	-	-
[Destruc] Destructoras de Papel	{1,9}	-	-	-	-
[Cub] Cubículos de Usuarios	{1,4}	{0,76}	{2,8}	-	-
[fib] Fibra Óptica	{0}	{1,9}	{2,8}	{3,3}	{3,1}

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[edificio] Inverna	{0}	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{0}	{2,6}	{2,5}	{3,3}	{3,4}

A nivel de los parámetros de seguridad, las calificaciones de los activos se han distribuido en cuatro fases: potencial, actual, objetivo, PILAR:

- [D] disponibilidad

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	{0}	{0}	{0}	{0}
[Impresión] Impresoras	{4,5}	{3,2}	{1,6}	{0,99}
[Backup] Respaldos	{0}	{0}	{0}	{0}
[Active Dir] Directorio Activo	{0}	{0}	{0}	{0}
[Tim] Gestor de Identidades	{5,4}	{3,9}	{2,2}	{1,8}

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	{0}	{0}	{0}	{0}
[ERP] Infor LN	{0}	{0}	{0}	{0}
[BDD] Bases de Datos	{0}	{0}	{0}	{0}
[Sist_op] Sistemas Operativos	{0}	{0}	{0}	{0}
[HW] Equipos	{7,2}	{5,7}	{4,2}	{3,6}
[pc] Equipos de usuarios	{5,4}	{4,1}	{2,4}	{1,8}
[rack_srv] Racks de Servidores	{7,2}	{5,7}	{4,2}	{3,6}
[Srv] Servidores de Centro de Datos	{0}	{0}	{0}	{0}
[Srv_intel] Servidores Intel Windows	{0}	{0}	{0}	{0}
[Sw] Switches	{0}	{0}	{0}	{0}
[COM] Comunicaciones	{5,4}	{3,6}	{2,2}	{1,9}
[Red_Lan] Red Lan	{5,4}	{3,3}	{2,0}	{1,8}
[Red Wifi] Red Inalámbrica	{5,4}	{3,4}	{2,0}	{1,9}
[firewall] Cortafuegos	{5,4}	{3,6}	{2,2}	{1,8}
[AUX] Elementos auxiliares	{5,4}	{4,0}	{2,3}	{1,9}
[Proy] Proyectores Digitales	{5,4}	{4,0}	{2,3}	{1,9}
[Destruc] Destructoras de Papel	{5,4}	{3,8}	{2,1}	{1,9}

[Cub] Cubículos de Usuarios	{4,8}	{3,3}	{1,6}	{1,4}
[fib] Fibra Óptica	{0}	{0}	{0}	{0}

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	{0}	{0}	{0}	{0}
[Cuarto_srv] Cuarto de Servidores	{0}	{0}	{0}	{0}

- [I] integridad de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	{6,3}	{4,5}	{3,7}	{2,5}
[Impresión] Impresoras	{6,8}	{5,2}	{4,5}	{3,0}
[Backup] Respaldos	{8,1}	{6,5}	{5,4}	{4,3}
[Active Dir] Directorio Activo	{7,2}	{5,5}	{4,7}	{3,4}
[Tim] Gestor de Identidades	{7,2}	{5,5}	{4,7}	{3,4}

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	{8,1}	{6,8}	{5,4}	{4,3}
[ERP] Infor LN	{8,1}	{6,8}	{5,4}	{4,3}
[BDD] Bases de Datos	{8,1}	{6,6}	{5,3}	{4,3}
[Sist_op] Sistemas Operativos	{6,8}	{5,7}	{3,6}	{3,2}
[HW] Equipos	{6,8}	{5,3}	{4,2}	{3,3}
[pc] Equipos de usuarios	{6,3}	{4,7}	{3,7}	{2,4}
[rack_srv] Racks de Servidores	{6,8}	{5,3}	{3,8}	{3,3}
[Srv] Servidores de Centro de Datos	{6,8}	{5,1}	{4,2}	{3,2}
[Srv_intel] Servidores Intel Windows	{6,8}	{5,1}	{4,2}	{3,2}
[Sw] Switches	{5,1}	{3,5}	{1,8}	{1,5}
[COM] Comunicaciones	{5,9}	{4,2}	{3,1}	{2,2}
[Red_Lan] Red Lan	{5,6}	{3,7}	{2,7}	{1,8}
[Red Wifi] Red Inalámbrica	{5,6}	{3,7}	{2,6}	{1,8}
[firewall] Cortafuegos	{5,9}	{4,2}	{3,1}	{2,2}
[AUX] Elementos auxiliares	{5,6}	{3,9}	{2,7}	{1,9}
[Proy] Proyectores Digitales	-	-	-	-
[Destruc] Destructoras de Papel	-	-	-	-
[Cub] Cubículos de Usuarios	{3,3}	{1,5}	{0,76}	{0,76}
[fib] Fibra Óptica	{5,6}	{3,9}	{2,7}	{1,9}

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{6,3}	{4,6}	{3,5}	{2,6}

- [C] confidencialidad de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	{6,3}	{4,7}	{3,4}	{2,5}
[Impresión] Impresoras	{8,1}	{6,6}	{5,5}	{4,2}
[Backup] Respaldos	{6,3}	{4,8}	{3,4}	{2,5}
[Active Dir] Directorio Activo	{6,3}	{5,0}	{3,5}	{2,5}
[Tim] Gestor de Identidades	{6,3}	{5,0}	{3,5}	{2,5}

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	{6,8}	{5,9}	{3,6}	{3,1}
[ERP] Infor LN	{6,8}	{5,9}	{3,6}	{3,1}
[BDD] Bases de Datos	{6,8}	{5,7}	{3,3}	{3,1}
[Sist_op] Sistemas Operativos	{6,8}	{5,8}	{3,4}	{3,1}
[HW] Equipos	{6,8}	{5,4}	{4,2}	{3,3}
[pc] Equipos de usuarios	{6,3}	{4,9}	{3,5}	{2,4}
[rack_srv] Racks de Servidores	{6,8}	{5,3}	{3,8}	{3,3}
[Srv] Servidores de Centro de Datos	{6,8}	{5,4}	{4,2}	{3,3}
[Srv_intel] Servidores Intel Windows	{6,8}	{5,4}	{4,2}	{3,3}
[Sw] Switches	{6,8}	{5,2}	{3,6}	{3,3}
[COM] Comunicaciones	{6,3}	{4,7}	{3,4}	{2,5}
[Red_Lan] Red Lan	{6,3}	{4,4}	{3,4}	{2,5}
[Red Wifi] Red Inalámbrica	{6,3}	{4,4}	{3,4}	{2,5}
[firewall] Cortafuegos	{6,3}	{4,7}	{3,3}	{2,5}
[AUX] Elementos auxiliares	{6,3}	{4,6}	{3,4}	{2,8}
[Proy] Proyectores Digitales	-	-	-	-
[Destruc] Destructoras de Papel	-	-	-	-
[Cub] Cubículos de Usuarios	{6,3}	{4,5}	{2,8}	{2,8}
[fib] Fibra Óptica	{6,3}	{4,6}	{3,4}	{2,8}

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{6,3}	{4,7}	{3,4}	{2,5}

- [A] autenticidad de los usuarios y de la información

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	{6,8}	{5,0}	{4,2}	{3,2}
[Impresión] Impresoras	{6,2}	{4,7}	{3,8}	{2,3}
[Backup] Respaldos	{6,8}	{5,2}	{4,3}	{3,2}
[Active Dir] Directorio Activo	{6,8}	{5,3}	{4,3}	{3,2}
[Tim] Gestor de Identidades	{6,8}	{5,3}	{4,3}	{3,2}

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	{6,8}	{5,5}	{4,2}	{3,3}
[ERP] Infor LN	{6,8}	{5,5}	{4,2}	{3,3}
[BDD] Bases de Datos	{6,8}	{5,2}	{4,2}	{3,3}
[Sist_op] Sistemas Operativos	{6,8}	{5,2}	{4,2}	{3,3}
[HW] Equipos	{6,8}	{5,2}	{4,3}	{3,2}
[pc] Equipos de usuarios	{6,8}	{5,2}	{4,3}	{3,2}
[rack_srv] Racks de Servidores	{6,2}	{4,6}	{3,2}	{2,7}
[Srv] Servidores de Centro de Datos	{6,8}	{5,1}	{4,2}	{3,2}
[Srv_intel] Servidores Intel Windows	{6,8}	{5,1}	{4,2}	{3,2}
[Sw] Switches	-	-	-	-
[COM] Comunicaciones	{6,8}	{5,1}	{4,0}	{3,3}
[Red_Lan] Red Lan	{6,8}	{4,9}	{3,9}	{3,2}
[Red Wifi] Red Inalámbrica	{6,8}	{4,9}	{3,9}	{3,2}
[firewall] Cortafuegos	{6,8}	{5,1}	{4,0}	{3,3}
[AUX] Elementos auxiliares	{6,8}	{5,0}	{3,7}	{3,3}
[Proy] Proyectores Digitales	-	-	-	-
[Destruc] Destructoras de Papel	-	-	-	-
[Cub] Cubículos de Usuarios	-	-	-	-
[fib] Fibra Óptica	{6,8}	{5,0}	{3,7}	{3,3}

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{6,8}	{5,1}	{4,2}	{3,3}

- [T] trazabilidad del servicio y de los datos

[IS] Servicios internos

activo	[potencial]	[current]	[target]	[PILAR]
[Email] Mensajería	{6,8}	{5,4}	{3,7}	{3,3}
[Impresión] Impresoras	{6,8}	{5,7}	{4,0}	{3,3}
[Backup] Respaldos	{6,8}	{5,7}	{3,8}	{3,4}
[Active Dir] Directorio Activo	{7,4}	{6,3}	{4,5}	{4,0}
[Tim] Gestor de Identidades	{7,4}	{6,3}	{4,5}	{4,0}

[E] Equipamiento

activo	[potencial]	[current]	[target]	[PILAR]
[SW] Aplicaciones	{6,8}	{6,0}	{3,9}	{3,3}
[ERP] Infor LN	{6,8}	{6,0}	{3,9}	{3,3}
[BDD] Bases de Datos	{6,8}	{5,8}	{3,7}	{3,3}
[Sist_op] Sistemas Operativos	{6,8}	{5,8}	{3,7}	{3,3}
[HW] Equipos	{6,8}	{5,8}	{3,9}	{3,3}
[pc] Equipos de usuarios	{6,8}	{5,8}	{3,9}	{3,3}
[rack_srv] Racks de Servidores	{6,8}	{5,3}	{3,8}	{3,3}
[Srv] Servidores de Centro de Datos	{6,8}	{5,4}	{3,7}	{3,3}
[Srv_intel] Servidores Intel Windows	{6,8}	{5,4}	{3,7}	{3,3}
[Sw] Switches	-	-	-	-

[COM] Comunicaciones	{6,8}	{5,5}	{3,6}	{3,2}
[Red_Lan] Red Lan	{6,8}	{5,0}	{3,4}	{3,2}
[Red Wifi] Red Inalámbrica	{6,8}	{5,0}	{3,4}	{3,2}
[firewall] Cortafuegos	{6,8}	{5,5}	{3,6}	{3,2}
[AUX] Elementos auxiliares	{6,8}	{5,3}	{3,6}	{3,1}
[Proy] Proyectores Digitales	-	-	-	-
[Destruc] Destructoras de Papel	-	-	-	-
[Cub] Cubículos de Usuarios	-	-	-	-
[fib] Fibra Óptica	{6,8}	{5,3}	{3,6}	{3,1}

[L] Instalaciones

activo	[potencial]	[current]	[target]	[PILAR]
[edificio] Inverna	-	-	-	-
[Cuarto_srv] Cuarto de Servidores	{6,8}	{5,5}	{3,8}	{3,4}

3.13 Identificación y valoración de salvaguardas

Para la identificación y valoración de salvaguardas es necesario considerar aquellas que son relevantes para lo que hay que proteger, considerando los siguientes aspectos:

1. El tipo de activos que se quiere proteger, ya que cada tipo se protege de una forma diferente.
2. Las amenazas a las que el activo requiere protección.
3. Si existen salvaguardas alternativas o adicionales.
4. Centrarse en los riesgos más importantes, esto dependerá de la zona de riesgo que PILAR evidencie.

Cabe señalar que existen diferentes tipos de protección prestados por las salvaguardas según (Amutio, 2012):

- [PR] Preventivo: Cuando se reducen las oportunidades de que un incidente ocurra. Ejemplo: Pruebas en pre-producción
- [CR] Correctivo: Después de ocurrirse el daño, se repara y se reducen los daños. Ejemplos: Gestión de incidentes.
- [DC] Detectivo: Al producirse un ataque, se notifica el suceso. Si bien no impide el ataque, permite que entren en operación otras medidas

que mitiguen la progresión del ataque. Ejemplos: anti-virus.

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas, en el presente proyecto se estimará un grado de eficacia real en cada caso y se empleará una escala de madurez dentro del proceso de gestión de la salvaguarda:

Tabla 19
Eficacia y madurez de las salvaguardas

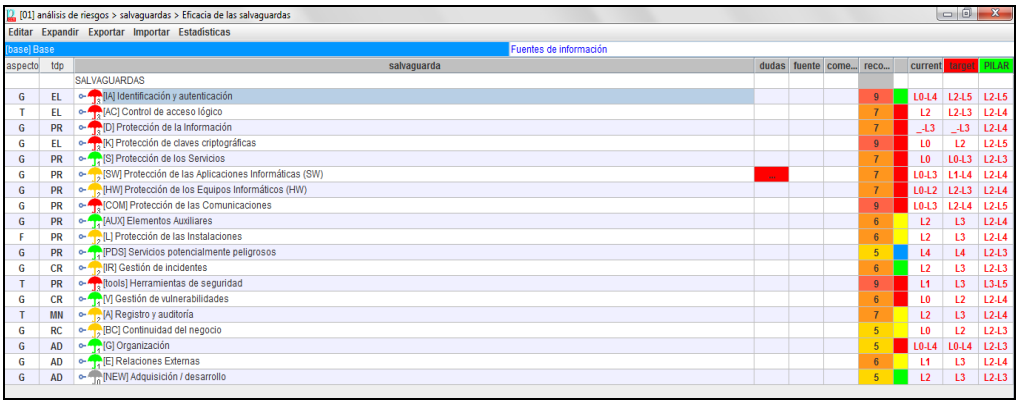
Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

También se debe recalcar que no todas las salvaguardas tienen la misma importancia, por lo cual se deben identificar en base a la tabla 20:

Tabla 20
Niveles de salvaguardas

Nivel	Peso	Significado
	Máximo peso	Crítica
	Peso alto	Muy importante
	Peso normal	Importante
	Peso bajo	Interesante

Con la ayuda de la herramienta, la figura 27 muestra la eficacia de las salvaguardas al aplicarse y con ello la reducción de los riesgos asociados:


[01] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] Base — Fuentes de información

aspecto	tdp	salvaguarda	dudas	fuente	come...	reco...	current	target	PILAR
		SALVAGUARDAS							
G	EL	[IA] Identificación y autenticación				9	L0-L4	L2-L5	L2-L5
T	EL	[AC] Control de acceso lógico				7	L2	L2-L3	L2-L4
G	PR	[D] Protección de la Información				7	_-L3	_-L3	L2-L4
G	EL	[K] Protección de claves criptográficas				9	L0	L2	L2-L5
G	PR	[S] Protección de los Servicios				7	L0	L0-L3	L2-L3
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)	...			7	L0-L3	L1-L4	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7	L0-L2	L2-L3	L2-L4
G	PR	[COM] Protección de las Comunicaciones				9	L0-L3	L2-L4	L2-L5
G	PR	[AUX] Elementos Auxiliares				6	L2	L3	L2-L4
F	PR	[L] Protección de las Instalaciones				6	L2	L3	L2-L4
G	PR	[PDS] Servicios potencialmente peligrosos				5	L4	L4	L2-L3
G	CR	[IR] Gestión de incidentes				6	L2	L3	L2-L3
T	PR	[tools] Herramientas de seguridad				9	L1	L3	L3-L5
G	CR	[V] Gestión de vulnerabilidades				6	L0	L2	L2-L4
T	MN	[A] Registro y auditoría				7	L2	L3	L2-L4
G	RC	[BC] Continuidad del negocio				5	L0	L2	L2-L3
G	AD	[G] Organización				5	L0-L4	L0-L4	L2-L3
G	AD	[E] Relaciones Externas				6	L1	L3	L2-L4
G	AD	[NEW] Adquisición / desarrollo				5	L2	L3	L2-L3

Figura 27 Eficacia de salvaguardas

Se identifica que deben aplicarse cuatro niveles de salvaguardas críticas debido a que su nivel es 9, es decir catastrófico siendo las siguientes:

- Identificación y autenticación
- Protección de claves criptográficas
- Protección de las comunicaciones
- Herramientas de seguridad

Es importante considerar que las salvaguardas que deben aplicarse se asocian con los controles de la Norma ISO 27002 utilizadas en la fase de situación actual, al cumplirse se fortalecerá el control interno de la Compañía.

La figura 28, muestra en porcentajes la situación actual de dominios de la Norma y también el objetivo que se espera conseguir aplicando las salvaguardas:

recom...		control	current	target	PILAR
		[27002:2013] Código de prácticas para los controles de seguridad de la información	34%	49%	57%
2		[5] Políticas de seguridad de la información	10%	50%	50%
7		[6] Organización de la seguridad de la información	50%	50%	35%
		[7] Seguridad relativa a los recursos humanos	n.a.	n.a.	
6		[8] Gestión de activos	38%	50%	48%
7		[9] Control de acceso	41%	38%	52%
9		[10] Criptografía	n.a.	n.a.	65%
6		[11] Seguridad física y del entorno	39%	50%	72%
9		[12] Seguridad de las operaciones	20%	50%	73%
9		[13] Seguridad de las comunicaciones	49%	50%	81%
7		[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	13%	50%	44%
6		[15] Relación con proveedores	30%	50%	81%
5		[16] Gestión de incidentes de seguridad de la información	50%	50%	68%
6		[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	17%	50%	74%
5		[18] Cumplimiento	50%	50%	61%

Figura 28 Porcentajes de cumplimiento de dominio ISO 27002

A continuación, se detalla de forma porcentual los controles de la Norma ISO 27002 con base al análisis de riesgos realizado:

[5] Políticas de seguridad de la información

control	R	[current]	[target]	[PILAR]
[5] Políticas de seguridad de la información	2	10%	10%	50%
[5.1] Directrices de gestión de la seguridad de la información	2	10%	10%	50%
[5.1.1] Políticas para la seguridad de la información	2	10%	10%	50%
[5.1.2] Revisión de las políticas para la seguridad de la información	2	10%	10%	50%

[6] Organización de la seguridad de la información

control	R	[current]	[target]	[PILAR]
[6] Organización de la seguridad de la información	7	50%	73%	35%
[6.1] Organización interna	7	50%	73%	69%
[6.1.1] Roles y responsabilidades en seguridad de la información	3	52%	76%	55%
[6.1.2] Separación de tareas	7	50%	50%	81%
[6.1.3] Contacto con las autoridades	3	50%	80%	80%
[6.1.4] Contacto con grupos de interés especial	5	50%	80%	80%
[6.1.5] Seguridad de la información en la gestión de proyectos	2	50%	80%	50%
[6.2] Los dispositivos móviles y el teletrabajo		n.a.	n.a.	0%
[6.2.1] Política de dispositivos móviles		n.a.	n.a.	n.a.
[6.2.2] Teletrabajo		n.a.	n.a.	n.a.

[7] Seguridad relativa a los recursos humanos

control	R	[current]	[target]	[PILAR]
[7] Seguridad relativa a los recursos humanos		n.a.	n.a.	
[7.1] Antes del empleo		n.a.	n.a.	0%
[7.1.1] Investigación de antecedentes		n.a.	n.a.	n.a.
[7.1.2] Términos y condiciones del empleo		n.a.	n.a.	n.a.
[7.2] Durante el empleo		n.a.	n.a.	0%
[7.2.1] Responsabilidades de gestión		n.a.	n.a.	n.a.
[7.2.2] Concienciación, educación y capacitación en seguridad de la información		n.a.	n.a.	n.a.
[7.2.3] Proceso disciplinario		n.a.	n.a.	n.a.
[7.3] Finalización del empleo o cambio en el puesto de trabajo		n.a.	n.a.	0%
[7.3.1] Responsabilidades ante la finalización o cambio		n.a.	n.a.	n.a.

[8] Gestión de activos

control	R	[current]	[target]	[PILAR]
[8] Gestión de activos	6	35%	67%	47%
[8.1] Responsabilidad sobre los activos	5	31%	71%	59%
[8.1.1] Inventario de activos	5	33%	71%	64%
[8.1.2] Propiedad de los activos	4	31%	71%	63%
[8.1.3] Uso aceptable de los activos	2	28%	70%	50%
[8.1.4] Devolución de activos		n.a.	n.a.	n.a.
[8.2] Clasificación de la información	6	40%	63%	82%
[8.2.1] Clasificación de la información	4	80%	80%	79%
[8.2.2] Etiquetado de la información	6	0%	45%	85%
[8.2.3] Manipulado de la información		n.a.	n.a.	n.a.
[8.3] Manipulación de los soportes		n.a.	n.a.	0%
[8.3.1] Gestión de soportes extraíbles		n.a.	n.a.	n.a.
[8.3.2] Eliminación de soportes		n.a.	n.a.	n.a.
[8.3.3] Soportes físicos en tránsito		n.a.	n.a.	n.a.

[9] Control de acceso

control	R	[current]	[target]	[PILAR]
[9] Control de acceso	7	41%	50%	52%
[9.1] Requisitos de negocio para el control de acceso	4	50%	73%	57%
[9.1.1] Política de control de acceso	4	50%	65%	64%
[9.1.2] Acceso a las redes y a los servicios de red	2	50%	80%	50%
[9.2] Gestión de acceso de usuario	7	54%	66%	70%
[9.2.1] Registro y baja de usuario	5	53%	80%	70%
[9.2.2] Provisión de acceso de usuario	3	50%	63%	60%

[9.2.3] Gestión de privilegios de acceso	7	61%	61%	79%
[9.2.4] Gestión de la información secreta de autenticación de los usuarios	6	60%	84%	70%
[9.2.5] Revisión de los derechos de acceso de usuario	4	50%	50%	70%
[9.2.6] Retirada o reasignación de los derechos de acceso	5	50%	58%	73%
[9.3] Responsabilidades del usuario	7			
[9.3.1] Uso de la información secreta de autenticación	7	0%	0%	0%
[9.4] Control de acceso a sistemas y aplicaciones	7	59%	60%	79%
[9.4.1] Restricción del acceso a la información	4	50%	50%	80%
[9.4.2] Procedimientos seguros de inicio de sesión	6	50%	50%	77%
[9.4.3] Sistema de gestión de contraseñas	7	85%	90%	85%
[9.4.4] Uso de utilidades con privilegios del sistema	3	50%	50%	74%
[9.4.5] Control de acceso al código fuente de los programas		n.a.	n.a.	n.a.

[10] Criptografía

control	R	[current]	[target]	[PILAR]
[10] Criptografía	9	0%	45%	75%
[10.1] Controles criptográficos	9	0%	45%	75%
[10.1.1] Política de uso de los controles criptográficos	4	0%	40%	65%
[10.1.2] Gestión de claves	9	0%	50%	86%

[11] Seguridad física y del entorno

control	R	[current]	[target]	[PILAR]
[11] Seguridad física y del entorno	6	39%	74%	72%
[11.1] Áreas seguras	6	50%	80%	69%
[11.1.1] Perímetro de seguridad física		n.a.	n.a.	n.a.
[11.1.2] Controles físicos de entrada		n.a.	n.a.	n.a.
[11.1.3] Seguridad de oficinas, despachos y recursos	5	50%	80%	80%
[11.1.4] Protección contra las amenazas externas y ambientales	6	50%	80%	78%
[11.1.5] El trabajo en áreas seguras	2	50%	80%	50%
[11.1.6] Áreas de carga y descarga		n.a.	n.a.	n.a.
[11.2] Seguridad de los equipos	6	29%	69%	75%
[11.2.1] Emplazamiento y protección de equipos	3	50%	80%	80%
[11.2.2] Instalaciones de suministro	6	50%	80%	77%
[11.2.3] Seguridad del cableado	6	50%	80%	82%
[11.2.4] Mantenimiento de los equipos	4	10%	80%	67%
[11.2.5] Retirada de materiales propiedad de la empresa	4	10%	50%	67%

[11.2.6] Seguridad de los equipos fuera de las instalaciones	4	10%	50%	62%
[11.2.7] Reutilización o eliminación segura de equipos	3	0%	80%	80%
[11.2.8] Equipo de usuario desatendido	6	50%	50%	87%
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia		n.a.	n.a.	n.a.

[12] Seguridad de las operaciones

control	**R**	**[current]**	**[target]**	**[PILAR]**
[12] Seguridad de las operaciones	9	35%	76%	73%
[12.1] Procedimientos y responsabilidades operacionales	5	19%	64%	65%
[12.1.1] Documentación de los procedimientos de operación	3	30%	63%	51%
[12.1.2] Gestión de cambios	5	18%	80%	67%
[12.1.3] Gestión de capacidades	3	10%	50%	77%
[12.1.4] Separación de los recursos de desarrollo, prueba y operación		n.a.	n.a.	n.a.
[12.2] Protección contra el software malicioso (malware)	9	20%	80%	82%
[12.2.1] Controles contra el código malicioso	9	20%	80%	82%
[12.3] Copias de seguridad	7	43%	80%	72%
[12.3.1] Copias de seguridad de la información	7	43%	80%	72%
[12.4] Registros y supervisión	7	50%	80%	76%
[12.4.1] Registro de eventos	6	50%	80%	74%
[12.4.2] Protección de la información de registro	6	50%	80%	90%
[12.4.3] Registros de administración y operación	2	50%	80%	50%
[12.4.4] Sincronización del reloj	7	50%	80%	88%
[12.5] Control del software en explotación	7	30%	83%	70%
[12.5.1] Instalación del software en explotación	7	30%	83%	70%
[12.6] Gestión de la vulnerabilidad técnica	6	33%	65%	64%
[12.6.1] Gestión de las vulnerabilidades técnicas	6	0%	65%	78%
[12.6.2] Restricción en la instalación de software	2	65%	65%	50%
[12.7] Consideraciones sore la auditoría de sistemas de información	5	50%	80%	80%
[12.7.1] Controles de auditoría de sistemas de información	5	50%	80%	80%

[13] Seguridad de las comunicaciones

control	R	[current]	[target]	[PILAR]
[13] Seguridad de las comunicaciones	9	35%	73%	80%
[13.1] Gestión de la seguridad de redes	9	47%	74%	82%
[13.1.1] Controles de red	5	43%	77%	73%
[13.1.2] Seguridad de los servicios de red	9	18%	65%	83%
[13.1.3] Segregación en redes	6	80%	80%	89%
[13.2] Intercambio de información	6	22%	72%	79%
[13.2.1] Políticas y procedimientos de intercambio de información	3	12%	50%	80%
[13.2.2] Acuerdos de intercambio de información	6	10%	80%	80%
[13.2.3] Mensajería electrónica	5	45%	85%	77%
[13.2.4] Acuerdos de confidencialidad o no revelación		n.a.	n.a.	n.a.

[14] Adquisición, desarrollo y mantenimiento de los sistemas de información

control	R	[current]	[target]	[PILAR]
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	7	20%	67%	45%
[14.1] Requisitos de seguridad en sistemas de información	7	17%	60%	66%
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	3	50%	80%	59%
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas	5	0%	54%	64%
[14.1.3] Protección de las transacciones de servicios de aplicaciones	7	0%	48%	76%
[14.2] Seguridad en el desarrollo y en los procesos de soporte	5	23%	74%	68%
[14.2.1] Política de desarrollo seguro		n.a.	n.a.	n.a.
[14.2.2] Procedimiento de control de cambios en sistemas	4	10%	80%	67%
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3	10%	80%	74%
[14.2.4] Restricciones a los cambios en los paquetes de software	2	50%	80%	50%
[14.2.5] Principios de ingeniería de sistemas seguros	3	10%	80%	80%
[14.2.6] Entorno de desarrollo seguro		n.a.	n.a.	n.a.
[14.2.7] Externalización del desarrollo de software	5	57%	72%	58%
[14.2.8] Pruebas funcionales de seguridad de sistemas		n.a.	n.a.	n.a.
[14.2.9] Pruebas de aceptación de sistemas	4	0%	50%	80%

[14.3] Datos de prueba		n.a.	n.a.	0%
[14.3.1] Protección de los datos de prueba		n.a.	n.a.	n.a.

[15] Relación con proveedores

control	R	[current]	[target]	[PILAR]
[15] Relación con proveedores	6	1%	9%	60%
[15.1] Seguridad en las relaciones con proveedores	6	1%	5%	62%
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores	6	2%	16%	54%
[15.1.2] Requisitos de seguridad en contratos con terceros	5	0%	0%	68%
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones	3	0%	0%	65%
[15.2] Gestión de la provisión de servicios del proveedor	6	2%	13%	57%
[15.2.1] Control y revisión de la provisión de servicios del proveedor	6	3%	27%	63%
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor	2	0%	0%	50%

[16] Gestión de incidentes de seguridad de la información

control	R	[current]	[target]	[PILAR]
[16] Gestión de incidentes de seguridad de la información	5	50%	80%	68%
[16.1] Gestión de incidentes de seguridad de la información y mejoras	5	50%	80%	68%
[16.1.1] Responsabilidades y procedimientos	5	50%	80%	60%
[16.1.2] Notificación de eventos de seguridad de la información	3	50%	80%	80%
[16.1.3] Notificación de puntos débiles de la seguridad	3	50%	80%	60%
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información	3	50%	80%	54%
[16.1.5] Respuesta a incidentes de seguridad de la información	4	50%	80%	70%
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	4	50%	80%	75%
[16.1.7] Recopilación de evidencias	3	50%	80%	80%

[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio

control	R	[current]	[target]	[PILAR]
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	6	17%	60%	74%
[17.1] Continuidad de la seguridad de la información	5	0%	46%	71%
[17.1.1] Planificación de la continuidad de la seguridad de la información	3	0%	50%	65%
[17.1.2] Implementar la continuidad de la seguridad de la información	5	0%	39%	68%
[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	3	0%	50%	80%
[17.2] Redundancia	6	33%	73%	77%
[17.2.1] Disponibilidad de los recursos de tratamiento de la información	6	33%	73%	77%

[18] Cumplimiento

control	R	[current]	[target]	[PILAR]
[18] Cumplimiento	5	12%	35%	60%
[18.1] Cumplimiento de los requisitos legales y contractuales	4	10%	31%	58%
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales	2	10%	10%	50%
[18.1.2] Derechos de propiedad intelectual (DPI)	3	17%	60%	53%
[18.1.3] Protección de los registros de la organización	3	0%	0%	55%
[18.1.4] Protección y privacidad de la información de carácter personal	3	23%	43%	73%
[18.1.5] Regulación de los controles criptográficos	4	0%	40%	58%
[18.2] Revisiones de la seguridad de la información	5	13%	40%	62%
[18.2.1] Revisión independiente de la seguridad de la información	5	20%	60%	70%
[18.2.2] Cumplimiento de las políticas y normas de seguridad	2	10%	10%	50%
[18.2.3] Comprobación del cumplimiento técnico	5	10%	50%	67%

Las salvaguardas a aplicarse serán a los dominios con menor porcentaje de cumplimiento, y por ende mayores riesgos.

A continuación, se describe un plan de acción de los principales controles que debe aplicarse sobre los riesgos identificados, con fechas de implementación y responsables a cargo.

PLAN DE ACCIÓN

DOMINIO: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: "Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes" (ISO 27000, 2012).

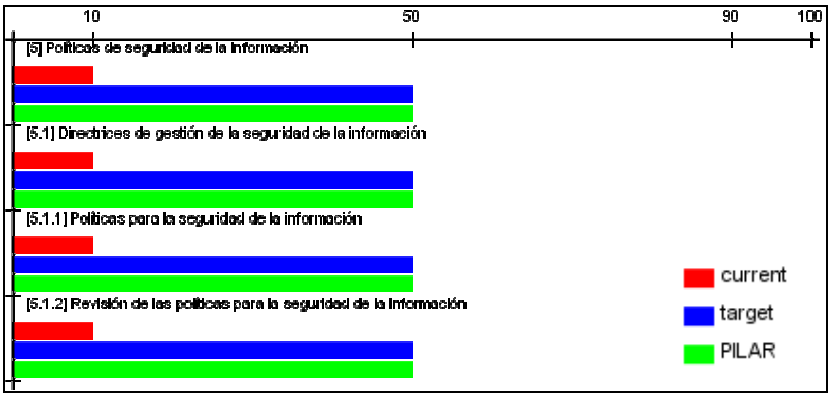


Figura 29 Resultado de PILAR - Dominio 5

Controles de la Normas ISO 27001:

Según (ISO 27001, 2013) establece los siguientes controles:

- "La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas

para la seguridad de la información".

- "Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos".

Salvaguardas a aplicarse:

La política de Seguridad de Información debe:

- [G.3.3.1] Estar aprobada por el responsable de seguridad.
- [G.3.3.2] Precisar lo que es uso adecuado y uso indebido.
- [G.3.3.3] Precisar la responsabilidad de las personas respecto de su cumplimiento y violación.
- [G.3.3.4] Todo el personal de la organización debe tener acceso a los documentos.
- [G.3.3.6] Ser revisadas con regularidad.

Plan de Acción:

Al Gerente de Seguridad de Información:

- Levantar el documento *Política de Seguridad de Información* describiendo el objetivo, alcance, responsabilidades y sanciones del no cumplimiento bajo el Reglamento Interno de la Compañía. Posterior debe ser revisado y aprobado por el Comité de Seguridad de Información y difundido vía correo e intranet corporativo para que todos los colaboradores pueden acceder al documento.

- Establecer campañas de concientización a los usuarios sobre el cumplimiento de la política.

El documento deberá ser revisado con una periodicidad anual o cuando existan cambios.

Fecha de Implementación: Inmediato

DOMINIO: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: "Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas" (ISO 27000, 2012).

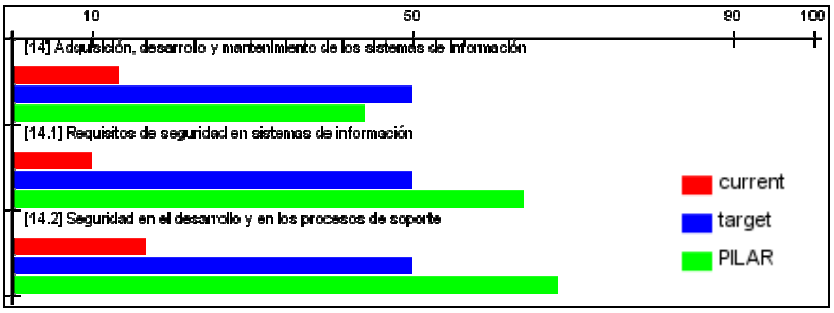


Figura 30 Resultado de PILAR - Dominio 14

Controles de la Normas ISO 27001:

Según (ISO 27001, 2013) establece los siguientes controles:

- Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.

- Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y

divulgación y modificaciones no autorizadas.

- Se debe proteger la información que provenga de las transacciones se los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.

Salvaguardas a aplicarse:

- [NEW.S.4.1] Se debe tener en cuenta los requisitos de control de acceso.
- [NEW.S.4.2] Se debe tener en cuenta los requisitos de identificación y autenticación.
- [14.2.2] Debe existir procedimientos de control de cambios en sistemas
- [14.2.3] Debe existir revisiones técnicas de las aplicaciones tras efectuar cambios en el sistema operativo.
- [14.2.4] Debe existir restricciones a los cambios en los paquetes de software.
- [NEW.SW.6.6.2] Debe existir una separación de funciones entre el personal que desarrolla y el personal encargado de producción.
- [14.2.9] Debe existir pruebas de aceptación de usuario para los sistemas que entran en producción por un tercero.

Plan de Acción:

A los Gerentes de Seguridad de Información y Mantenimiento Sistemas:

- Definir e implantar un procedimiento de control de cambios a programas y parametrizaciones, a fin de garantizar que todas las modificaciones sean autorizadas y aprobadas por las Gerencias.

- Establecer un procedimiento para la gestión de cambios en todos los aplicativos que forman parte de producción, establecer un único mecanismo de recepción de requerimientos, formatos de documentación, etapas de cambios a programas definidos y entregables.

- Solicitar pruebas retrospectivas de aceptación de usuarios para las fases entregadas, identificando que las versiones instaladas en los aplicativos no se han modificado desde su puesta en marcha, establecer un plan de pruebas y firmar la aceptación de pruebas.

- Implementar un control de revisión con frecuencia y responsable definidos que se vea reflejado en documentación (informes, actas) el cual certifique que todas las modificaciones realizadas a objetos, fuentes y módulos han sido realizadas conforme al procedimiento.

Dicho control debe ser archivado en el departamento para posibilitar consultas futuras y comprobar que se llevó a cabo.

Fecha de Implementación: septiembre del 2017.

DOMINIO: GESTIÓN DE LOS ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA CONTINUIDAD DEL NEGOCIO

Objetivo: “La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización” (ISO 27000, 2012).

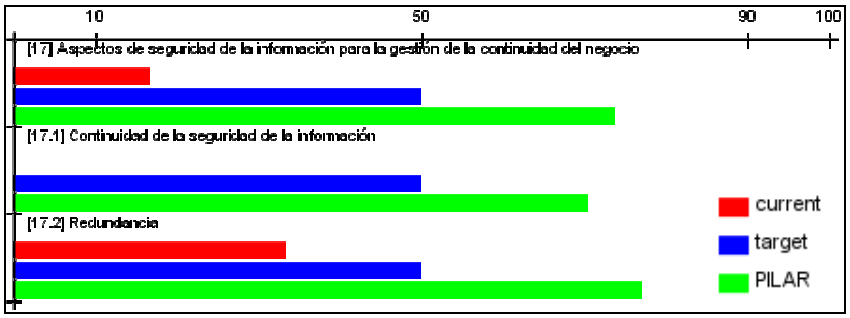


Figura 31 Resultado de PILAR - Dominio 17

Controles de la Normas ISO 27001:

Según (ISO 27001, 2013) establece los siguientes controles:

- La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, Ejemplo: Durante una crisis o desastre.

- La organización deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

- La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.

Salvaguardas a aplicarse:

- [BC.BIA] Se debe realizar un análisis de impacto (BIA).
- [BC.BIA.2] Se debe identificar los activos involucrados en los procesos críticos.

- [BC.BIA.3] Se deben establecer objetivos de recuperación para cada proceso crítico (RTO).
- [BC.BIA.4] Se deben establecer objetivos de recuperación para cada información crítica (RPO).
- [BC.DRP] Se debe generar un Plan de Recuperación de Desastres (DRP).
- [BC.1.2.3] Se debe realizar pruebas y los incidentes detectados deben ser analizados como si se hubieran producido sobre el sistema base.
- [17.2.1] Debe existir redundancia que garantice disponibilidad de los recursos de tratamiento de la información.

Plan de Acción:

Al Comité de Seguridad de Información:

Documentar y formalizar un Plan de Continuidad del Negocio, aprobado por las Direcciones de toda la Compañía, tomando como referencia los siguientes puntos:

- Identificar los procesos críticos de negocio y determinar las aplicaciones y equipos que soportan esos procesos.

- Definir las estrategias y períodos de recuperación.

- Determinar las responsabilidades del personal de sistemas y de los usuarios.

- Mantener un convenio formal con un centro de procesamiento de datos alterno como respaldo, en caso de ser la estrategia adoptada.

- Describir los procedimientos de recuperación, señalando los activadores, responsables, tiempos y demás asuntos pertinentes.

- Probar el plan antes de oficializarlo para verificar su viabilidad, así las

pruebas serán útiles para ayudar a determinar el grado de eficacia de dicho plan y proveerá entrenamiento al personal involucrado en la ejecución de los procedimientos en caso de un desastre.

- Difundir el plan, para hacer conocer a todo el personal sobre el plan de recuperación en cada área, esto reduciría la demora y confusión inherentes en toda recuperación en caso de un desastre.

- Determinar el mecanismo, las actividades y responsables para actualizar el plan de manera periódica.

Fecha de Implementación: diciembre del 2018.

3.14 Análisis de impacto y riesgo residual

Posterior de haber aplicado salvaguardas y una medida de la madurez del proceso de gestión, el impacto y el riesgo se ha modificado desde un valor potencial a un valor residual.

La figura 32, muestra los resultados del impacto residual, después de aplicar recomendaciones de las salvaguardas:

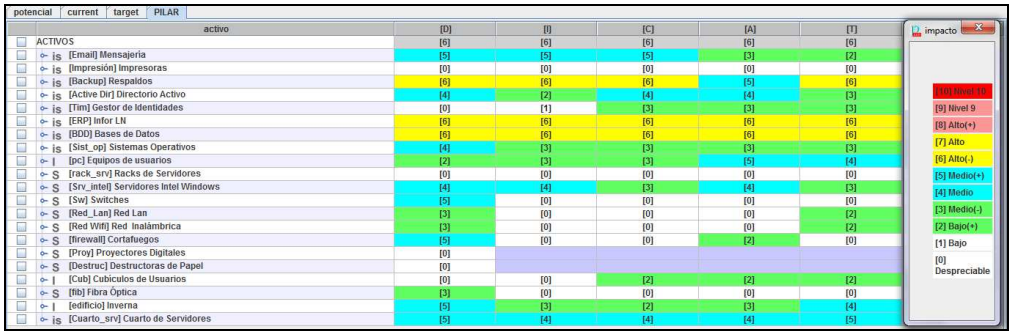


Figura 32 Análisis de impacto residual

La figura 33, muestra los resultados del riesgo residual, después de aplicar recomendaciones de las salvaguardas:

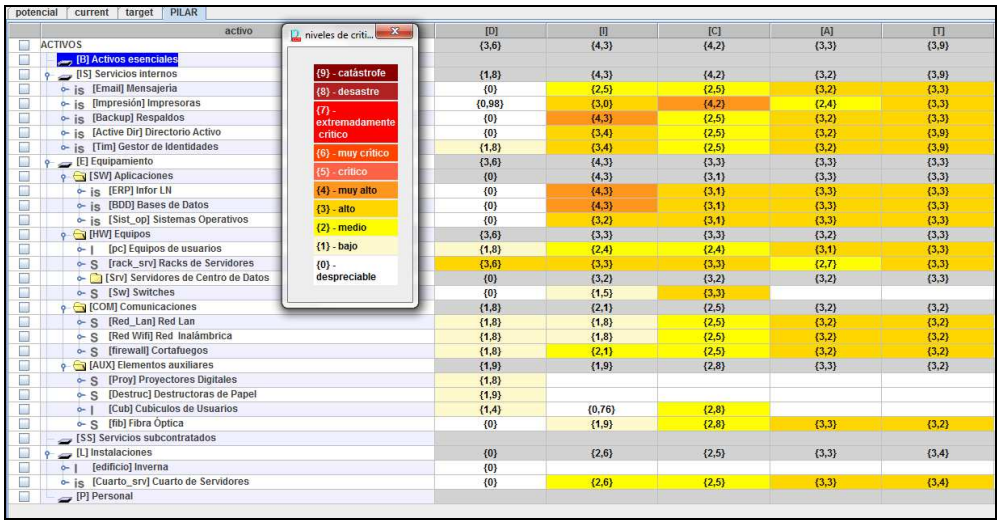


Figura 33 Análisis de riesgo residual

Como se puede observar en la figura 34, el nivel de evolución de los dominios de la Norma ISO 27002, tras aplicarse las recomendaciones de salvaguardas:

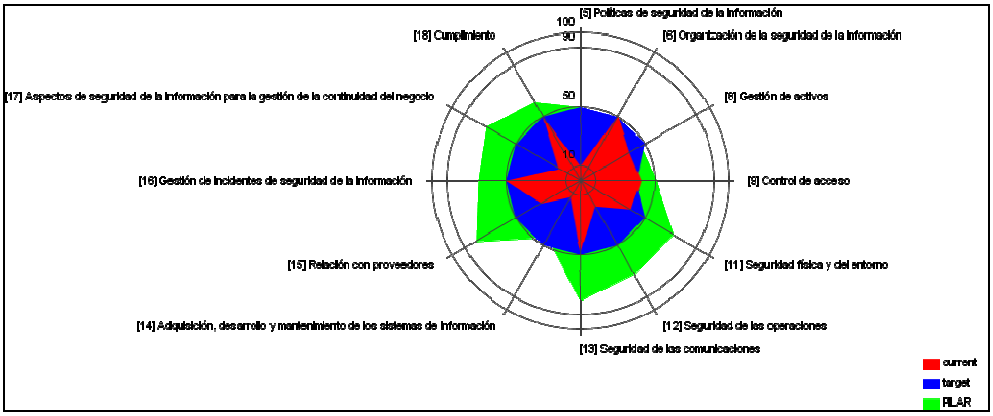


Figura 34 Fases de evolución de Norma ISO 27002

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se evaluó la situación actual de Seguridad de Información en el departamento de Tecnología e Información aplicando la Norma ISO 27000; el proyecto se complementó con la metodología propuesta denominada MAGERIT, y se automatizó el análisis utilizando el software PILAR.

- Se identificó que los activos de información críticos/sensibles son el ERP Corporativo Infor LN y Bases de Datos; al no aplicarse las salvaguardas correspondientes, podrían afectarse por amenazas que al materializarse degradarían a los activos de información.

- Se determinó que los siguientes dominios de la norma ISO 27001: Política de Seguridad de la Información, Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información y Gestión de los Aspectos de la Seguridad de la Información para la Continuidad del Negocio, carecen de controles; debido a que la Compañía está formalizando la Política de Seguridad Corporativa y también el desconocimiento de una adecuada gestión de riesgos para el mantenimiento de los sistemas y la continuidad de las operaciones en caso de incidentes.

- Se estableció que los riesgos se materializan a causa de las amenazas y vulnerabilidades; sin embargo, realizando un análisis de riesgos permitió identificar los riesgos de mayor importancia y que afectan la Seguridad de la Información de la Compañía.

4.2 Recomendaciones

- Implementar los controles de la Norma ISO 27000 que presenten mayores deficiencias en la Compañía con base al plan de acción propuesto, con la finalidad de fortalecer la Seguridad de Información de la Compañía.

- Aplicar las salvaguardas mencionadas con el fin de proteger los activos de información de amenazas y mitigar riesgos identificados, estableciendo un plan de remediación con fechas a corto, mediano y largo plazo y de suma importancia asignar responsables de la ejecución.

- Adquirir una herramienta que permita realizar análisis de riesgos a fin de automatizar el trabajo de gestión de amenazas y vulnerabilidades, reduciendo la necesidad del capital humano, errores involuntarios y tiempo requeridos, para generar una mejora continua y aumentar el nivel de madurez en términos de Seguridad de Información de la Compañía.

- Proyectar la generación de un Sistema de Gestión de Seguridad de Información SGSI, para que la Compañía diseñe, implante, y mantenga un conjunto de procesos para gestionar de manera eficiente la accesibilidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información y minimizando los riesgos en el proceso de tratamiento.

BIBLIOGRAFÍA

Academy 27001, A. (2016). *Qué es norma ISO 27001*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001

Aguilera, L. (2010). *Seguridad Informática* (Vol. 1). (E. S.A., Ed.) Madrid, España: ISBN 978-84-9771-657-4.

Aguirre, J. J. (2013). Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la Ofrenda. Pereira: Publicación Nro. 0058A284.

Amutio, M. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* (Vol. 1). Madrid, España: Ministerio de Hacienda y Administraciones Públicas. doi:NIPO: 630-12-171-8

Cappuccio, V. (2009). *Seguridad Informática*. Obtenido de http://audisistemas2009.galeon.com/productos2229098.html

González, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (Vol. 3). Madrid, España: NIPO: 630-12-171-8.

Gutiérrez, C. (2013). *ISO/IEC 27002:2013 y los cambios en los dominios de control.* Obtenido de http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

Isaca. (2011). *Auditoría de Sistemas. Protección de Activos de Información (Basado en Riesgo)*. Obtenido de http://www.isaca.org/Blogs/282270/archive/2011/04/27/Protecci%C3%B3ndeActivosdeInformaci%C3%B3n.aspx

ISO 27000. (2012). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/iso27000.html

ISO 27000, P. (2012). *Sistema de Gestión de Seguridad de la Información*. Obtenido de Términos de Uso Información: http://www.iso27000.es/

ISO 27001. (2013). *Norma Internacional ISO/IEC 27001* (2 ed.).

Mañas, J. (2012). *Entorno de análisis de riesgos*. Obtenido de http://www.ar-tools.com/es/training/audea.html

Mifsud, E. (2012). *Seguridad de la Información*. Obtenido de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Molina, M. (2015). *Propuesta de un Plan de Gestión de Riesgos de Tecnología Aplicado en la Escuela Superior Politécnica del Litoral.* Madrid, España.

Moncayo, E. (2014). Diseño de un Sistema de Gestión en Control y Seguridad basado en la norma Basc para la Empresa de Transportes y Servicios Asociados Sytsa Cía. Ltda. Pichincha: ESPE-048199.

Morán, E. (2012). *Reflexiones en voz alta sobre el SGSI - 27001*. Obtenido de https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/

Portal Administración Electrónica, 2. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WVJ5wus1-00

Ramos, A. (2012). *Magerit v3 y 17 nuevas guías STIC*. Obtenido de http://www.securitybydefault.com/2012/10/ccn-cert-magerit-v3-y-17-nuevas-guias.html

Rosero, E. (2014). Análisis de Riesgos de la Seguridad de la Red de Área Local (Lan) de la Matriz de la Contraloría General del Estado, Provincia de Pichincha. Pichincha: T-UCE-0011-81.

Sotelo, M. J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. *COMTEL 2012 IV Congreso Internacional de Computación y Telecomunicaciones.*

Symantc. (2016). *Glosario de Seguridad.* Obtenido de https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad